In het vizier

Hoe digitaal weerbaar zijn bedrijven in België en Luxemburg?

Cybersecurity rapport 2025

Terwijl consumenten en bedrijven profiteren van de digitale transformatie om wonen, werken en leven comfortabeler te maken, nemen de aanvalsvlakken voor cybercriminelen nagenoeg synchroon toe. Hoewel dat besef bij ondernemers nadrukkelijk aanwezig is, legt onze jaarlijkse bevraging verschillende verbeterpunten en onzekerheden bloot. Gezien het grote belang van kennisdeling, verheugt het mij opnieuw dat 193 beslissingsnemers uit België en Luxemburg hun bevindingen hebben gedeeld. Ik wens u bij het lezen van ons rapport veel inspiratie en nieuwe inzichten toe!

Raf Peeters
VP Cybersecurity and Networking
bij Proximus NXT

Inhoudstafel

De resultaten in vogelvlucht

33%

De impact is het grootst op het vlak van operationele data, met een stijging van 19% in 2023 naar 33% in 2024.

25%

Een kwart van de getroffen bedrijven ondervond reputatieschade.

25%

25% van de respondenten geven aan slachtoffer te zijn geweest van een cybersecurityincident – een daling van 5% ten opzichte van 2023 (30%). Toch blijft het aandeel aanzienlijk. Bij grote ondernemingen ligt dit percentage zelfs hoger, namelijk op 38%.

40%

40% van de respondenten had te maken met werkonderbrekingen. Die hinder bleef wel meestal beperkt tot minder dan een week.

60%

Bijna 60% van de kmo's weet helemaal niet of niet zeker of ze moeten voldoen aan de NIS2-regelgeving.

De belangrijkste bevindingen

1 Bedrijven tonen vandaag een groter bewustzijn rond cyberbeveiliging. Waar veel ondernemingen vroeger niet met zekerheid konden zeggen of ze al dan niet het slachtoffer waren van hackers, klinkt het vandaag overtuigder. Bedrijven met meer dan 2.000 werknemers hebben volgens onze bevraging zelfs volledige zekerheid bereikt.

2 Bijna 40% van de respondenten getuigt over een tekort aan gespecialiseerd cyberbeveiligingspersoneel, wat wijst op een kloof tussen de beoogde en de in realiteit aanwezige expertise.

3 Voor het derde opeenvolgende jaar verwacht meer dan 40% van de respondenten een toegenomen aantal cyberbeveiligingsincidenten of een grotere impact van dergelijke calamiteiten.

“Opvallend is dat veel bedrijven verwachten dat de tijd van zeer grote stijgingen van de cyberbeveiligingsbudgetten achter de rug ligt, al blijft de meerderheid van de ondernemingen gewag maken van een stijging van de budgetten.”

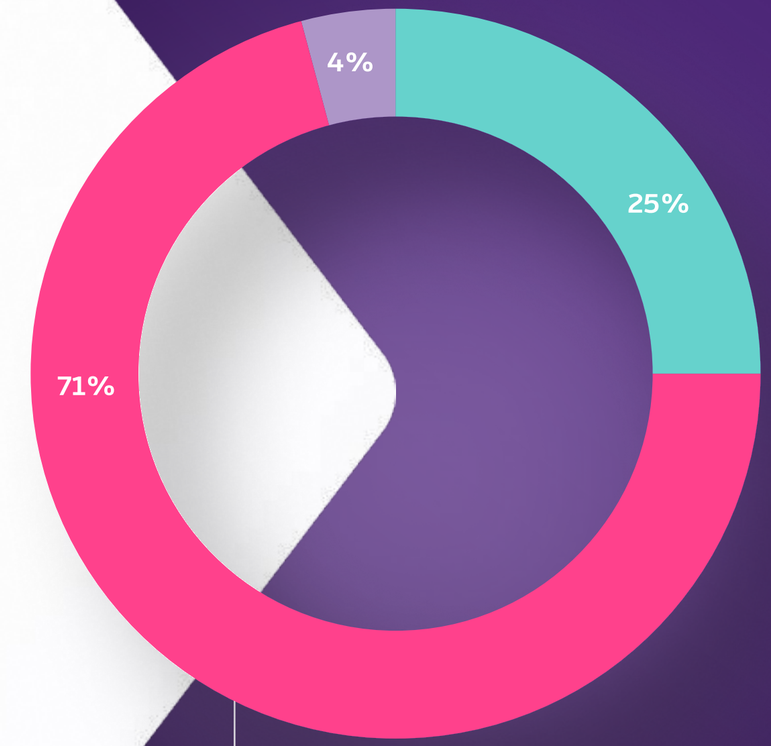
Wouter Vandenbussche,
Cybersecurity Services Lead bij Proximus NXT

Hoofdstuk 1

Cybersecurityincidenten

Of het nu gaat om het financieel afpersen van bedrijven, om politieke motieven of het verwerven van gevoelige data, het aantal wereldwijde cybersecurityincidenten neemt jaar na jaar toe. Het Wereld Economisch Forum wijst bovendien op een toenemende complexiteit van het cyberlandschap, wat diepgaande en verstrekkende gevolgen heeft voor elke organisatie.

Exact een kwart van de respondenten geeft aan dat hun bedrijf het voorbije jaar af te rekenen had met een cybersecurityincident. Een aanval raakte daarbij aan de vertrouwelijkheid, de integriteit of beschikbaarheid van informatie, of leidde tot productiviteitsverlies, wettelijke gevolgen, reputatieschade, dataverlies of andere nadelige gevolgen.



Heeft uw bedrijf de afgelopen 12 maanden te maken gehad met een of meer cybersecurityincidenten?

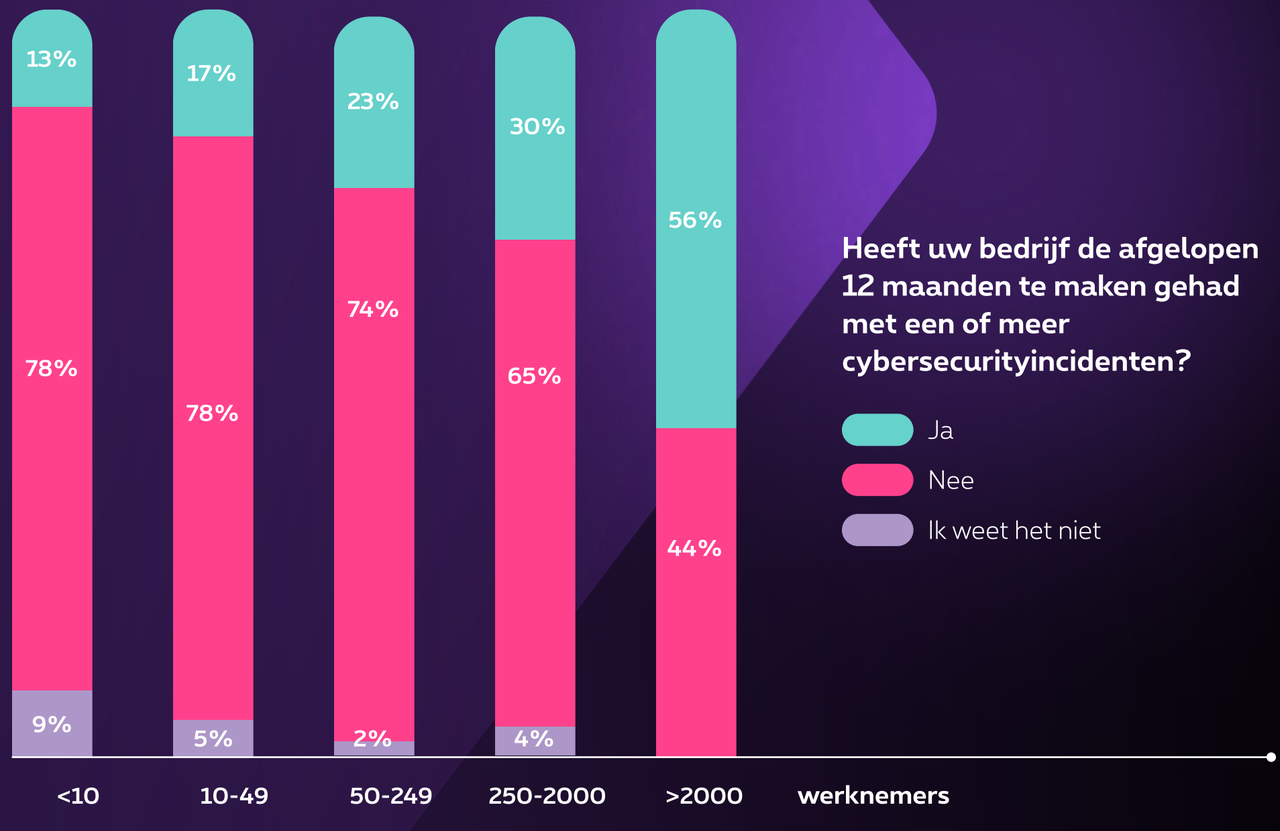
- Ja
- Nee
- Ik weet het niet

Leestip: Topexperts delen zeven Cybersecurity trends en -dreigingen voor 2025.

Grote bedrijven zijn vaker doelwit

Heeft uw bedrijf de afgelopen 12 maanden te maken gehad met een of meer cybersecurityincidenten?

- Ja
- Nee
- Ik weet het niet

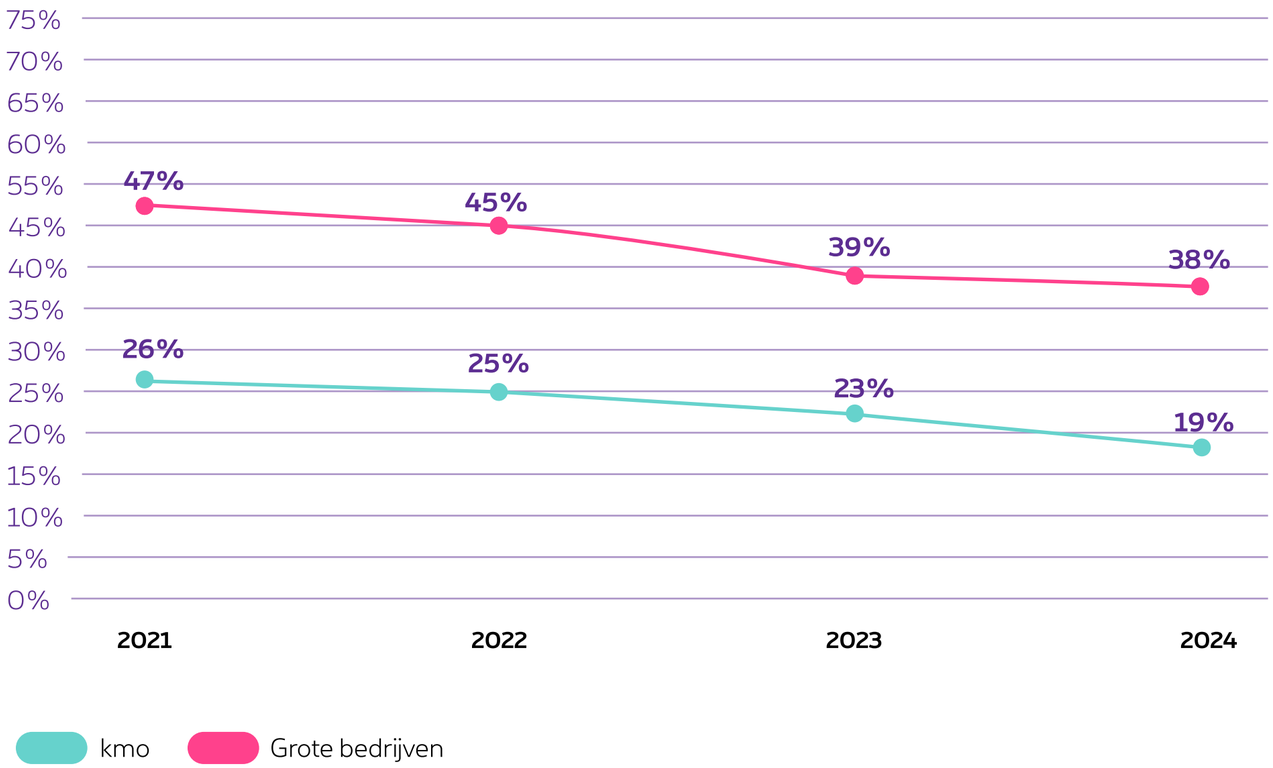


Heeft uw bedrijf de afgelopen 12 maanden te maken gehad met een of meer cybersecurityincidenten?

- Ja
- Nee
- Ik weet het niet

Grote bedrijven zijn vaker doelwit

Bedrijven met meer dan 250 medewerkers (38%) rapporteren immers vaker cybersecurityincidenten dan kleinere of middelgrote organisaties (19%). Van de zeer grote ondernemingen met meer dan 2000 medewerkers gaf 56% aan de afgelopen 12 maanden een incident te hebben meegemaakt, vergeleken met 45% in 2023.



Veel ondernemingen konden vroeger niet met zekerheid zeggen of ze al dan niet het slachtoffer waren van hackers. Vandaag zijn ze meer overtuigd."

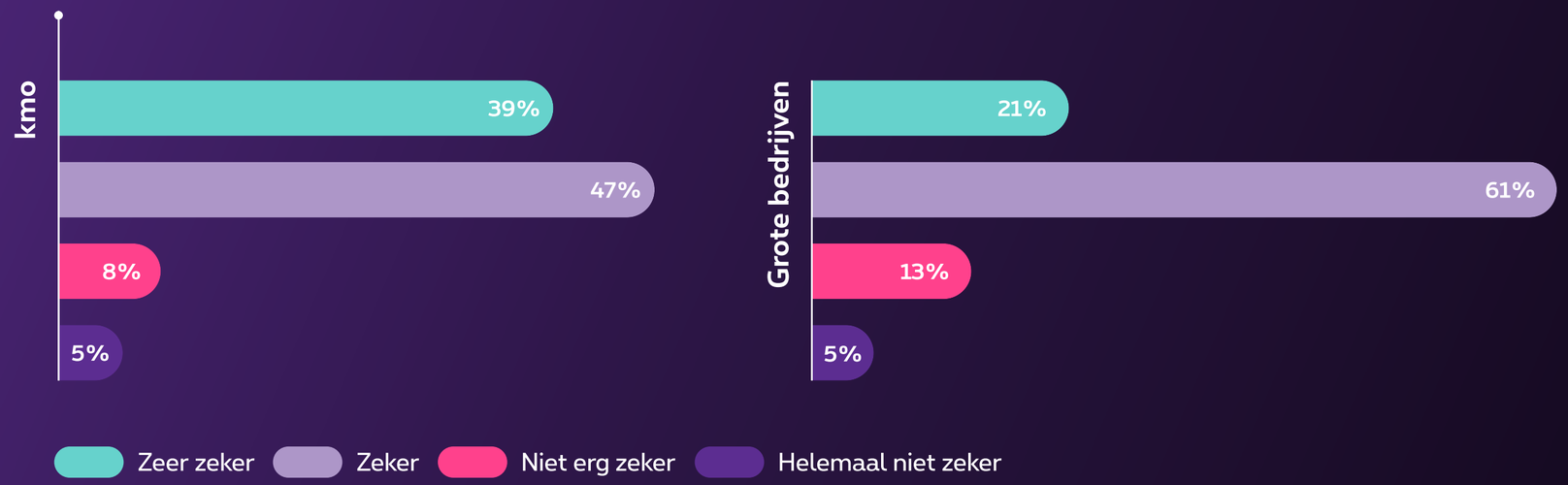
Wouter Vandenbussche,
Cybersecurity Services Lead

Beoordelings- en detectievertrouwen

De meeste organisaties (85%) zijn ervan overtuigd dat ze in de afgelopen 12 maanden geen enkel cyberbeveiligingsincident hebben meegemaakt. Wie beweert het voorbije jaar niet geraakt te zijn, is daar dus ook van overtuigd. Kmo's worden mogelijk minder geviseerd door cybercriminelen. Bovendien heeft de IT-verantwoordelijke in kleinere organisaties vaak meer zicht op het geheel, wat het veiligheidsgevoel kan versterken. Grotere ondernemingen, met complexere infrastructuur, uiten meer voorbehoud.

De bedrijven die aangeven niet te zijn geconfronteerd met een cyberbeveiligingsincident, etaleren veel vertrouwen in hun vermogen om aanvallen te detecteren. Grote bedrijven met uitgebreidere middelen en toegewijde teams tonen de grootste zelfzekerheid op dat vlak

Hoe groot is uw zekerheid dat er de afgelopen 12 maanden geen cybersecurity-incidenten binnen uw bedrijf hebben plaatsgevonden?

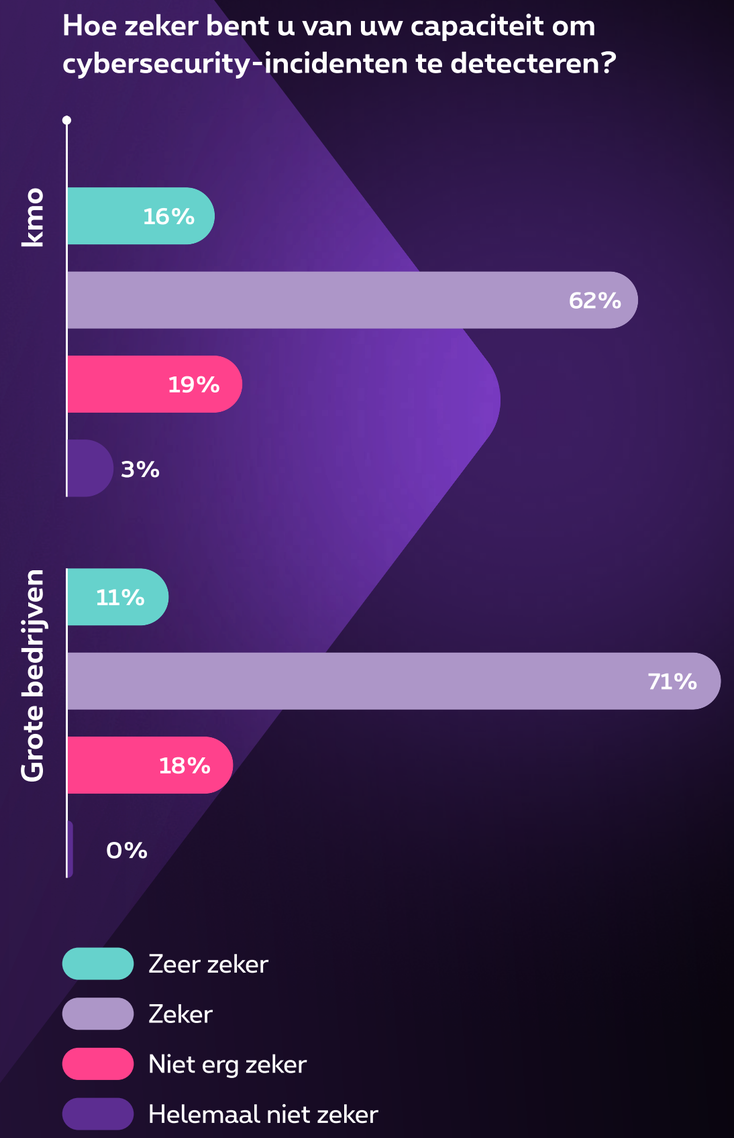


Aantal gedetecteerde incidenten

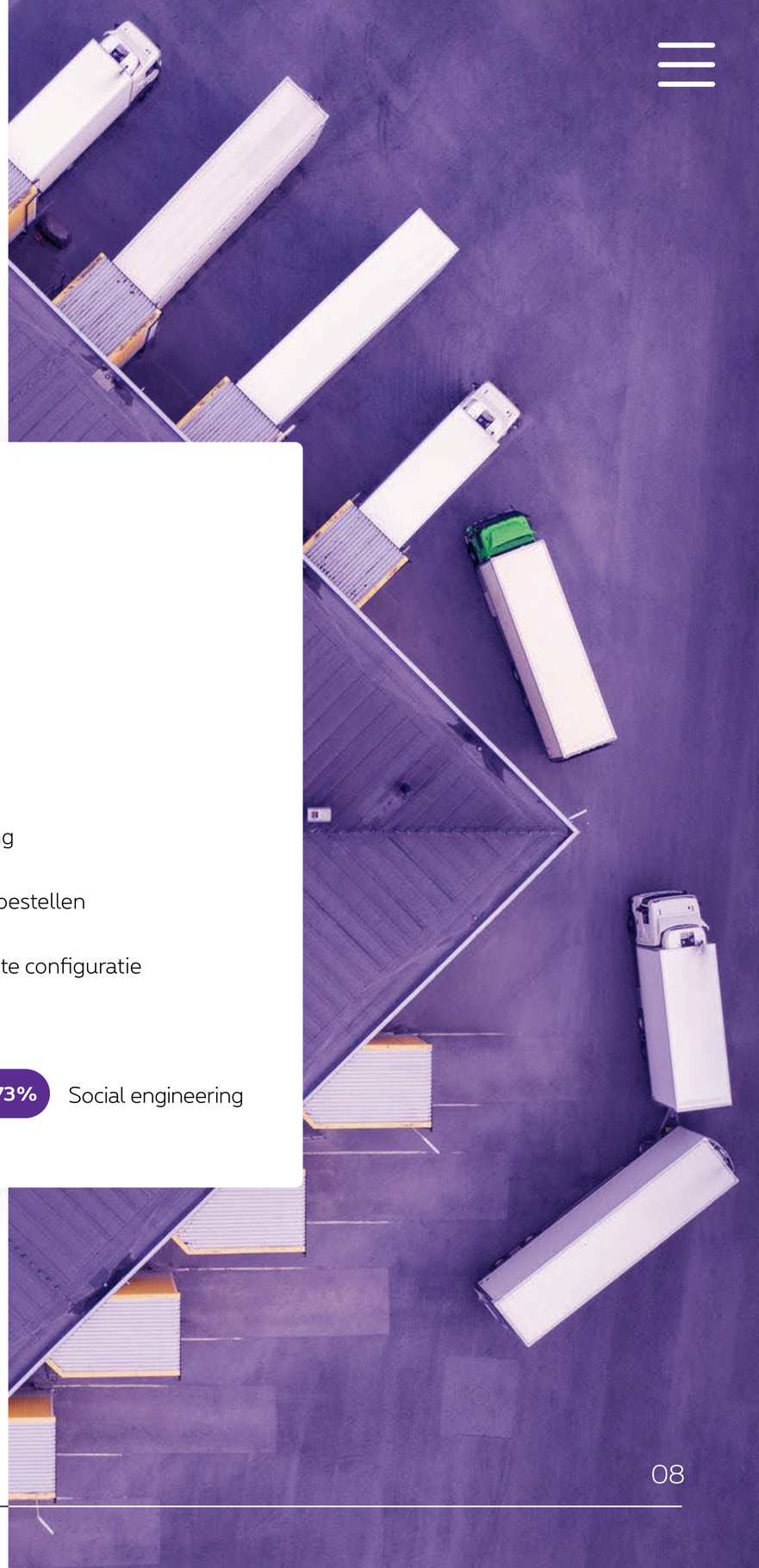
Het aantal gedetecteerde incidenten loopt sterk uiteen. Bij een overgrote meerderheid gaat het om een beperkt aantal: 81% meldt maximaal 5 gevallen.

Soorten incidenten

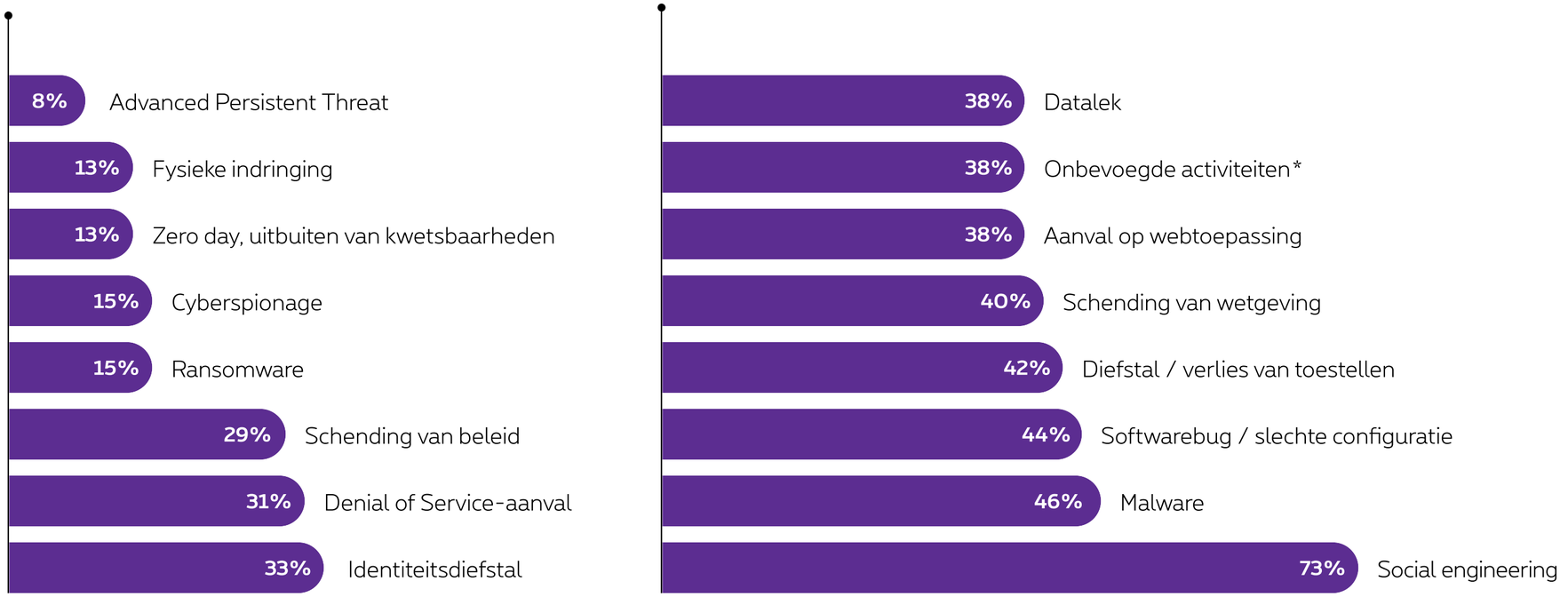
Vorig jaar klikte volgens het Cloud and Threat Report van Netskope elke maand wereldwijd meer dan acht op de duizend werknemers op een phishinglink, goed voor een stijging van 190% ten opzichte van 2023. Het toont aan dat criminelen vaak misbruik maken van een gebrek aan waakzaamheid om bedrijven te treffen.



De door ons bevraagde ondernemingen onderschrijven die bevinding, aangezien social engineering-aanvallen, zoals phishing, hen het vaakst treffen (73%). Op de tweede plaats prijkt malware (46%). Softwarebugs en foute configuraties (44%) vervolledigen de top drie.



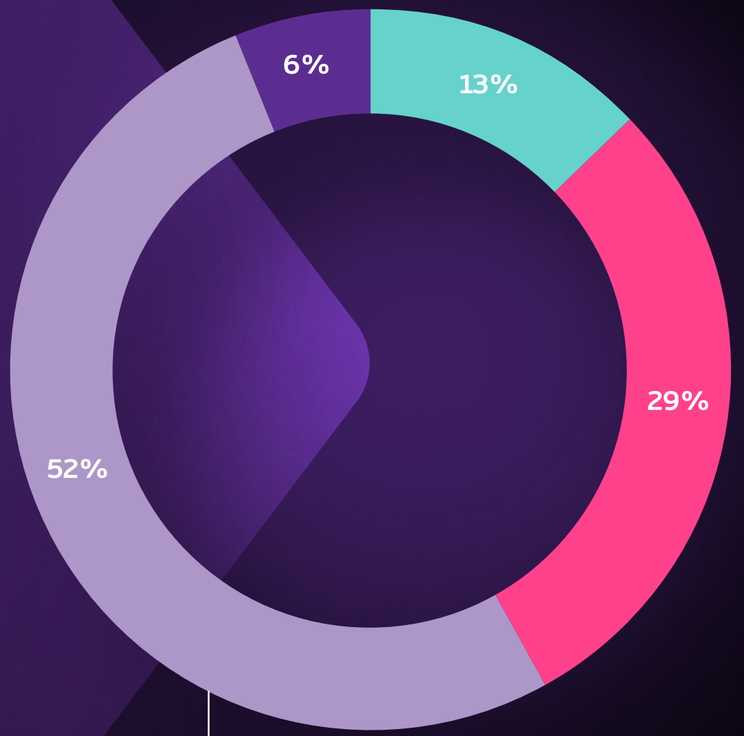
Welke types incidenten vonden plaats binnen uw organisatie?



*Onbevoegde activiteiten, zoals onbevoegde toegang tot informatiesystemen en netwerken, of het ongeoorloofd installeren of gebruiken van softwaretoepassingen

Intentioneel. Of toch niet?

81% van de organisaties beschouwt de gedetecteerde incidenten als opzettelijk. Verrassender is dat 65% getuigt van incidenten die per ongeluk plaatsvonden. Die vaststelling vraagt om extra behoedzaamheid voor bedreigingen van binnenuit. Een sterk toezicht op gebruikersidentiteiten en -rechten moet ervoor zorgen dat medewerkers niet nodeloos toegang krijgen tot gevoelige informatie of kritieke applicaties. Het is ook raadzaam om configuraties te monitoren en waar nodig bij te sturen.



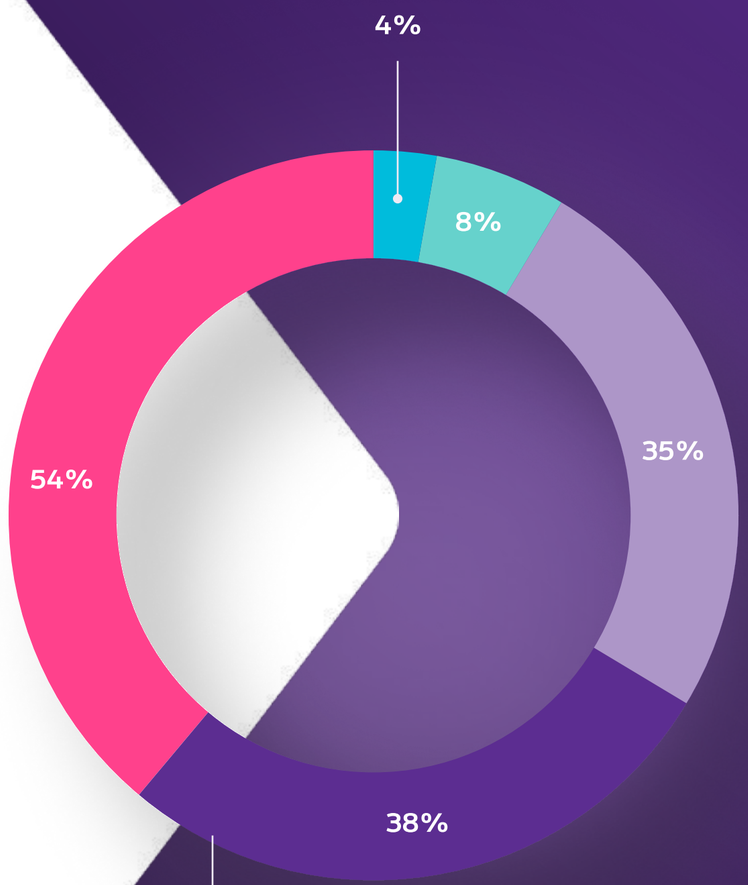
De incidenten die zich voordeden waren:

- Accidenteel
- Opzettelijk
- Zowel accidenteel als opzettelijk
- Ik weet het niet

Hoofdstuk 2

De impact van de incidenten

Van de directiekamer tot het militaire strijdtoneel: geen enkele omgeving bleef het voorbije jaar gevrijwaard van cyberaanvallen. Cyberbeveiligingsincidenten treffen apparaten zoals laptops, desktops en/of mobiele apparaten (54%). Netwerk- en cloudinfrastructuur vormt eveneens vaak het doelwit (38%).



Op welke fysieke assets was er een impact?

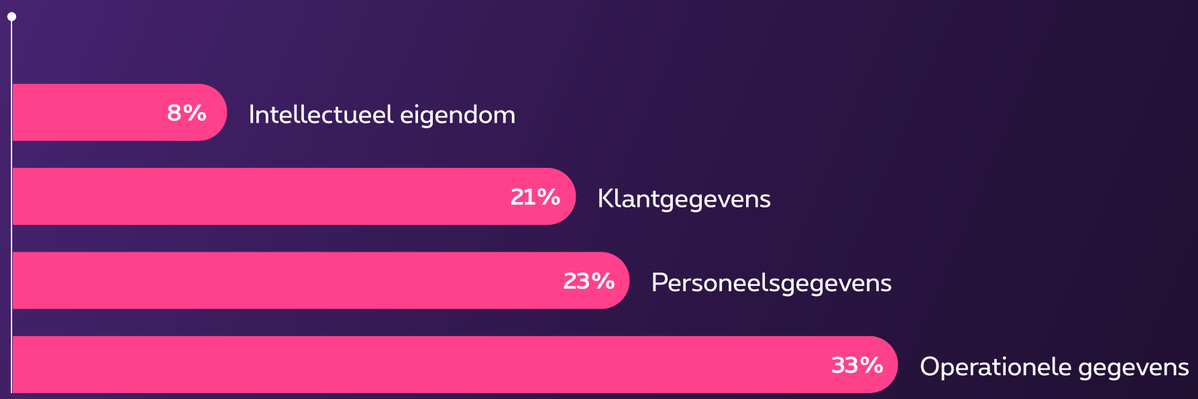
- Machines
- Kantoorapparatuur
- Cloudinfrastructuur, servers
- Netwerkinfrastructuur
- Laptops, desktops, mobiele toestellen

Digitale en fysieke assets

Aanvallen blijven niet zonder gevolgen voor de operationele bedrijfsdata (33%), werknemersdata (23%) en klanteninformatie (21%). Het is opvallend dat de impact op operationele bedrijfsdata een sterke stijging laat zien van 19% in 2023 naar 33% in 2024.

Respondenten meldden nog andere incidenten, zoals het in naam van hun bedrijf of persoon versturen van frauduleuze facturen, onbevoegde toegang tot e-mailaccounts, het aanvallen van laptops via de server en de verstoring van applicaties.

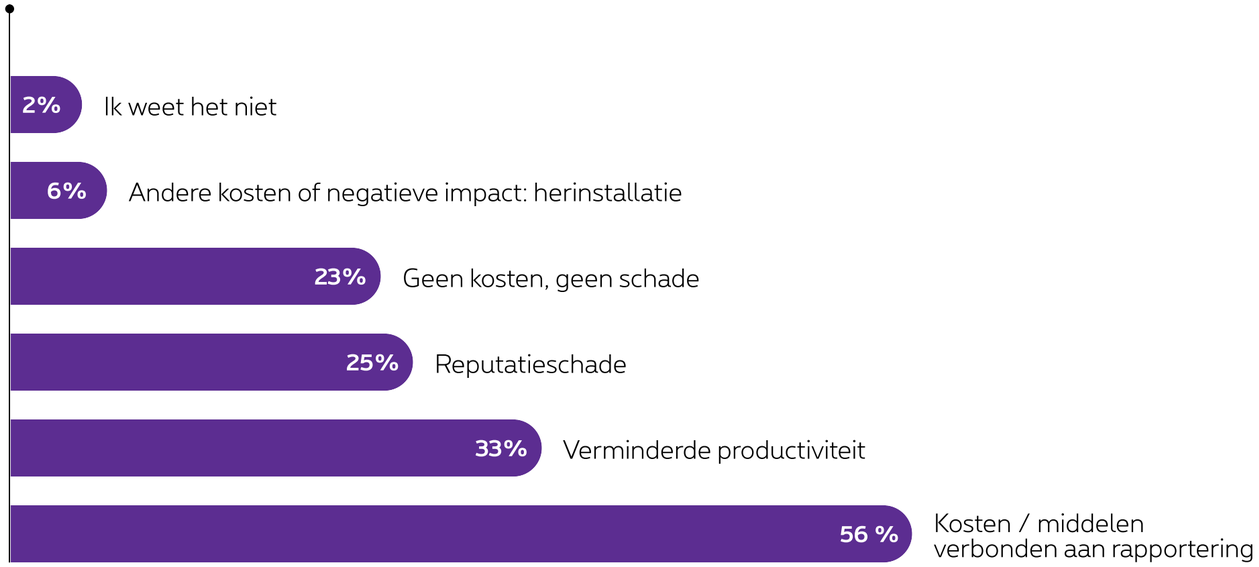
Welke digitale assets zijn getroffen?



Kosten en schade

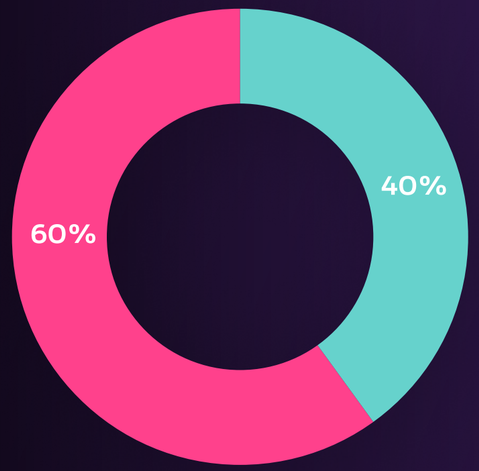
Effectieve rapportering vormt een cruciaal onderdeel binnen de bestrijding van cybercriminaliteit. De meldingsplicht bij incidenten vormt een essentieel onderdeel van zowel de GDPR- als de NIS2-wetgeving. Dat gaat evenwel ook gepaard met een kostenplaatje. Meer dan de helft van de respondenten noemen de interne en externe melding van incidenten zelfs het vaakst als belangrijkste kostenpost na een incident. Een derde van de bevraagden wijst op gedaalde productiviteit, terwijl één op vier reputatieschade aanstipt.

Wat was de impact van het (de) cybersecurityincident(en) op uw bedrijf in de afgelopen 12 maanden?



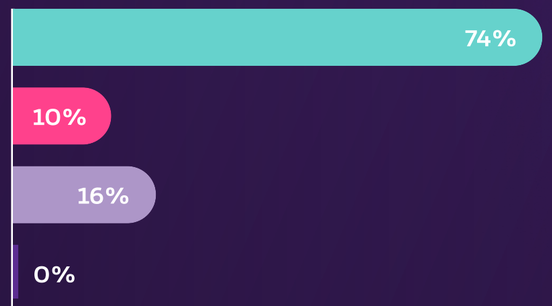
Aanslag op productiviteit

Vier op tien respondenten ondervonden werkonderbrekingen als gevolg van een cybersecurityincident. In driekwart van de gevallen kon maximaal 25% van de medewerkers tijdelijk niet aan de slag na een incident. Bij bijna een zesde van de bedrijven was meer dan de helft van het personeelsbestand noodgedwongen buiten strijd. Hoewel de meeste verstoringen binnen één dag van de baan waren, kampten ook veel bedrijven met een meerdaagse productiviteitsterugval.



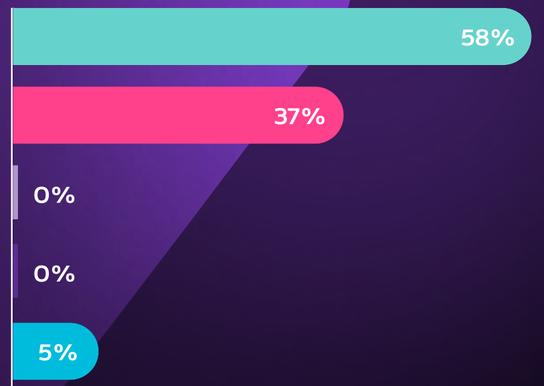
Hebben cybersecurity-incidenten ervoor gezorgd dat uw medewerkers niet konden werken?

- Ja
- Nee



Hoeveel procent van de medewerkers kon niet meer werken als gevolg van het meest ernstige incident?

- < 25%
- 25% - 50%
- 50% - 75%
- 75% - 100%



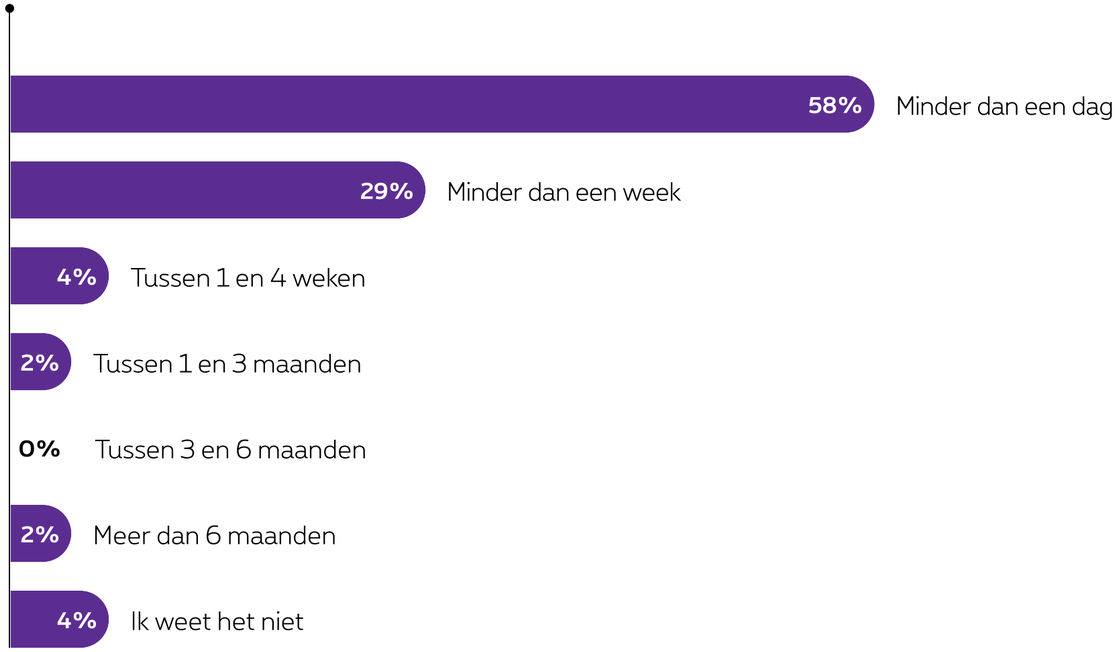
Hoe lang konden de medewerkers niet werken als gevolg van het meest ernstige incident?

- 1 dag
- Tussen 1 dag en 7 dagen
- Tussen 1 en 2 weken
- Meer dan 2 weken
- Ik weet het niet

Herstel en veerkracht

Het vermogen om snel te herstellen van cyberincidenten draagt bij tot de digitale weerbaarheid van een onderneming. Wanneer een organisatie haar activiteiten binnen een korte tijdsspanne weer op de rails krijgt, blijft de operationele impact doorgaans gering. Bij het leeuwendeel van de respondenten die het voorbije jaar een incident ondervond, gebeurde het herstel van de technische infrastructuur snel. In 58% van de gevallen volstond minder dan een dag. Een derde van de organisaties had enkele dagen tot een week nodig. Bij 4% nam het herstel meer dan een maand in beslag.

Hoeveel tijd kostte het om de technische infrastructuur na het ernstigste incident volledig weer operationeel te krijgen?



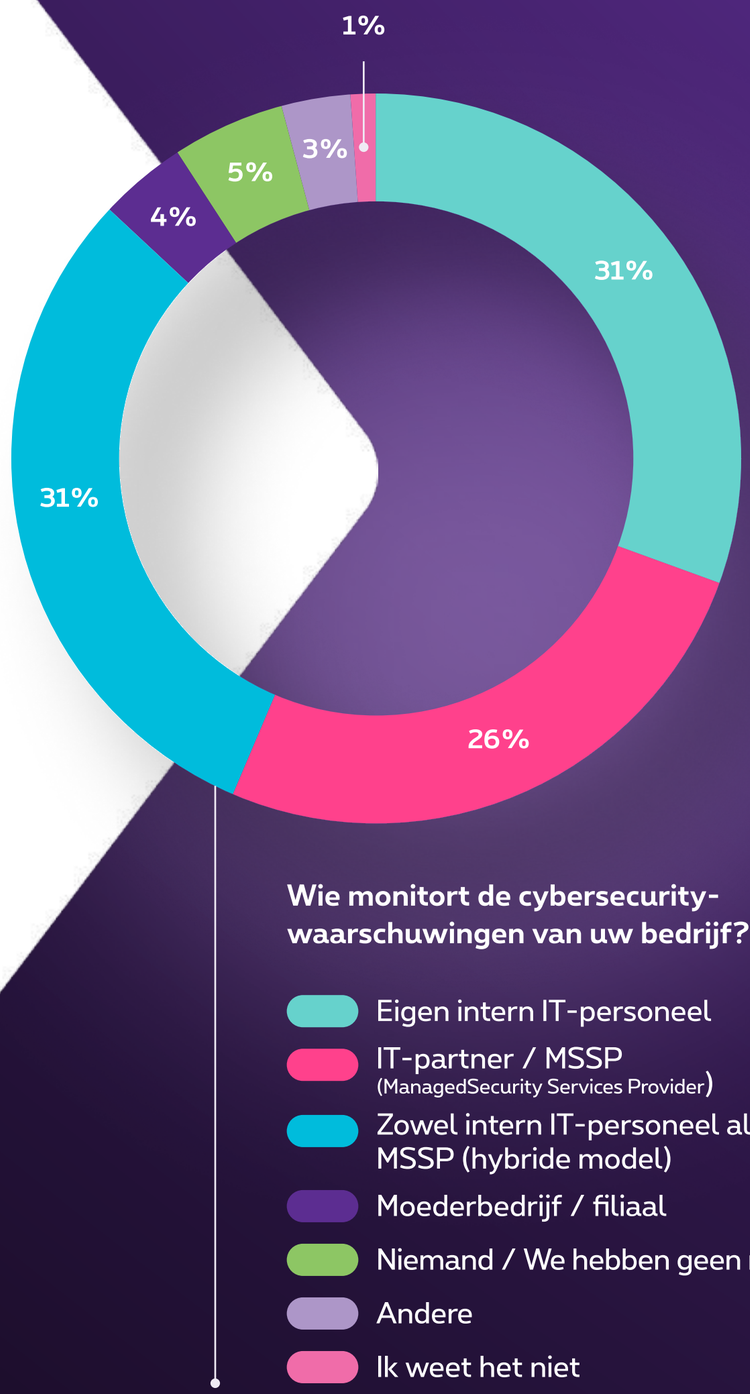
Hoofdstuk 3

Cybersecuritymaturiteit en strategie

Cybersecuritymaturiteit verwijst naar de paraatheid en capaciteit van een organisatie om zich te verdedigen tegen cyberdreigingen en te reageren op cyberincidenten. Het gaat zowel om het proces, het menselijk handelen binnen een organisatie als de weerbaarheid van de technologieën.

Monitoring door derden

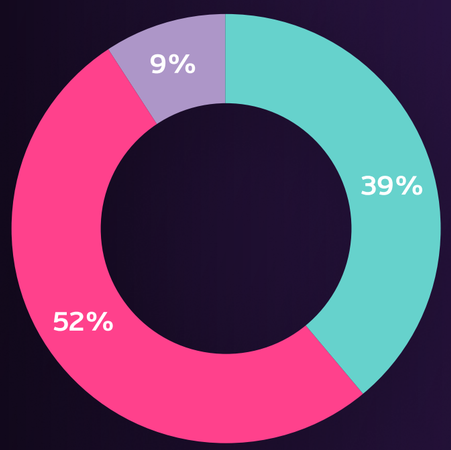
Veel organisaties verkiezen een hybride aanpak of vertrouwen op interne IT-medewerkers voor het monitoren van cyberbeveiliging. Dat wijst op een voorkeur voor het behouden van enige mate van controle. Ongeveer een kwart van de bedrijven besteedt de bewaking van cyberbeveiliging volledig uit aan een IT-partner of managed security service provider (MSSP). Dergelijke externe dienstverleners die een breed scala aan securitydiensten aanbieden, vormen een aantrekkelijke optie voor organisaties om hun cyberbeveiliging te verbeteren, zonder die intern te moeten beheren. 57% van de organisaties doet een beroep op zo'n derde partij.



ICT-afdeling en personeel

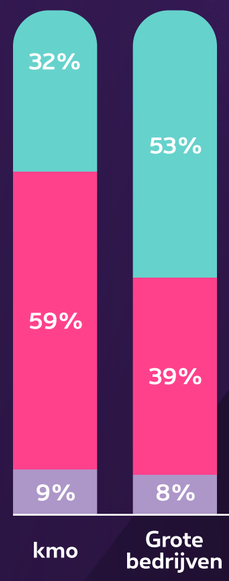
Het onderzoek laat een gemengd beeld zien wat de beschikbaarheid van gespecialiseerd cyberbeveiligingspersoneel betreft. Hoewel de meeste bedrijven vinden dat ze over voldoende personeel beschikken, ziet een significant aantal ook tekorten, terwijl bijna 10% die inschatting zelf niet kan maken.

Tekort aan IT-personeel
Vooral de grotere bedrijven ervaren een tekort aan gespecialiseerd personeel op hun beveiligingsafdelingen. Daartegenover staat dat amper een derde van de kmo's zijn huidige samenstelling onvoldoende acht. 60% van de kmo's gaf aan geen problemen te zien op het vlak van cybersecuritypersoneel, wat aanzienlijk meer is dan de grote bedrijven (39%).



Heeft uw bedrijf een tekort aan gespecialiseerde mensen op de beveiligingsafdeling?

- Ja
- Nee
- Ik weet het niet



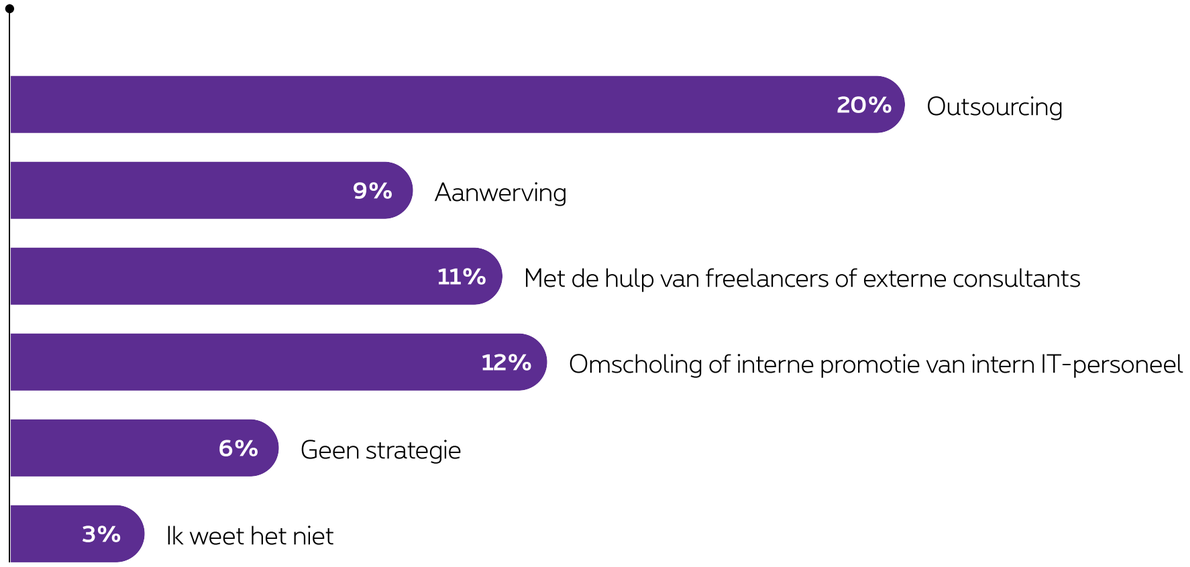
Heeft uw bedrijf een tekort aan gespecialiseerde mensen op de beveiligingsafdeling?

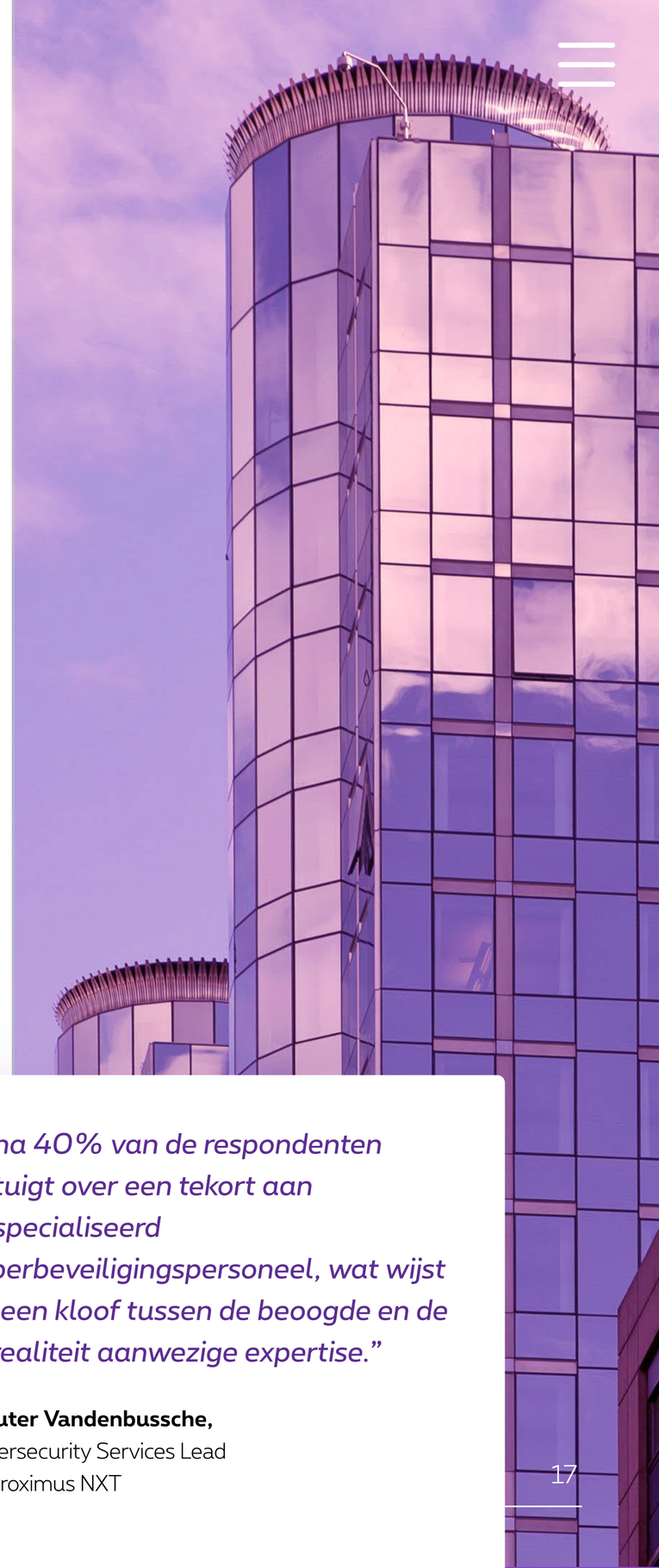
- Ja
- Nee
- Ik weet het niet

Kloof aan expertise dichten

Bedrijven putten uit een breed scala van strategieën om de kloof tussen de beschikbare kennis en vereiste vaardigheden op het vlak van cybersecurity te overbruggen. Outsourcing geniet de meeste bijval, gevolgd door het bijscholen van intern personeel en het inzetten van freelancers of consultants. Werving blijft een noodzakelijke strategie, hoewel die pas de vierde plaats bekleedt. Het is opvallend en tegelijk zorgwekkend dat bijna 1 op de 10 organisaties geen plan van aanpak heeft uitgetekend of zich niet bewust is van de noodzaak van zo'n plan.

Hoe zal u de vaardigheidskloof op uw beveiligingsafdeling dichten?





"Bijna 40% van de respondenten getuigt over een tekort aan gespecialiseerd cyberbeveiligingspersoneel, wat wijst op een kloof tussen de beoogde en de in realiteit aanwezige expertise."

Wouter Vandenbussche,
Cybersecurity Services Lead
bij Proximus NXT

Cybersecuritystrategie

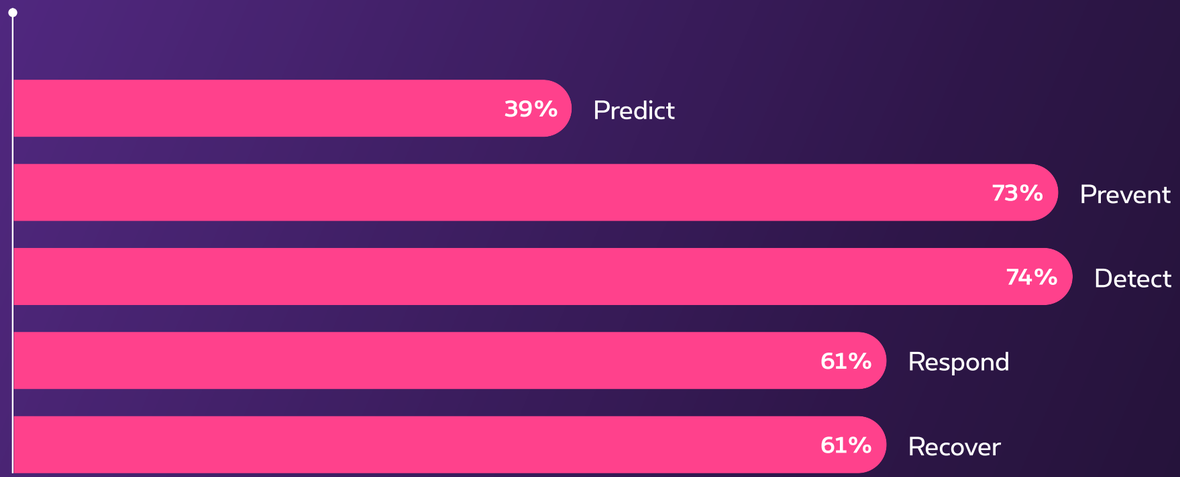
Een gedegen strategie op het vlak van cybersecurity is onontbeerlijk om dreigingen zowel proactief als reactief aan te pakken. Het NIST Cybersecurity Framework sluit daar naadloos op aan. Die richtlijn, ontwikkeld door het National Institute of Standards and Technology (NIST), helpt organisaties om hun cyberbeveiliging te verbeteren. Het raamwerk omvat op zijn beurt zes stadia: Identify, Protect, Detect, Respond, Recover en Govern. De maturiteit in de voorspellingsfase (Identify) ligt duidelijk het laagst. Het betekent dat veel bedrijven nog een verbeterslag kunnen maken in het inschatten van potentiële dreigingen. De IT-beslissingsnemers blijken vooral tevreden over het vermogen van hun organisatie om incidenten te voorkomen en te detecteren.

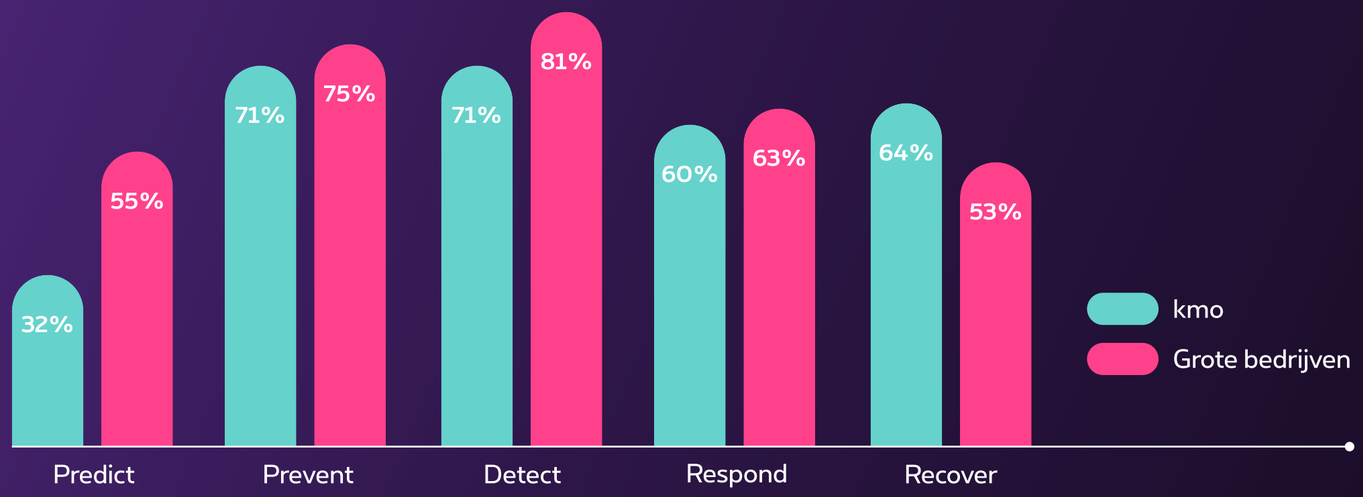
Proximus NXT helpt het volledige potentieel van data te ontsluiten dankzij zijn oplossingen en expertise op het vlak van connectiviteit, data en AI, beveiliging en clouddiensten. De ondersteuning binnen elke fase van de Data Life Cycle stelt bedrijven en organisaties in staat om te navigeren door een complex digitaal landschap, het datapotentieel te maximaliseren en groeikansen te benutten.

Data Life Cycle Management (DLM) geldt als een belangrijk raamwerk voor effectief gegevensbeheer gedurende de gehele levenscyclus.

- **Collect:** Verzamel gegevens uit verschillende bronnen, zoals klantinteracties, financiële transacties, productgegevens en operationele statistiekenren.
- **Connect:** Verbind en integreer gegevens uit verschillende bronnen tot een samenhangende dataset.
- **Transport & Store:** Analyseer de gegevens om inzichten te verkrijgen, trends te identificeren en prestaties te evalueren.
- **Process & Compute:** **Maak** de data schoon, en transformeer en organiseer ze om ze klaar te maken voor analyse.
- **Analyseren:** Verkrijg waardevolle inzichten uit verwerkte gegevens om zakelijke beslissingen te onderbouwen.
- **Samenwerken:** Gebruik samenwerkingstools tijdens de gehele datalevenscyclus om kennisdeling, efficiëntie en innovatie te verbeteren.

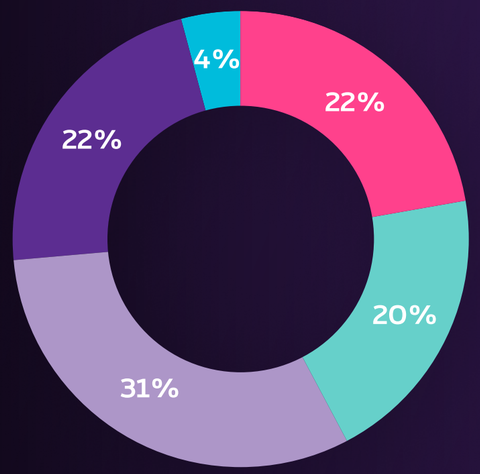
Als uw bedrijf een cyberbeveiligingsstrategie heeft, wat is dan de huidige stand van zaken?





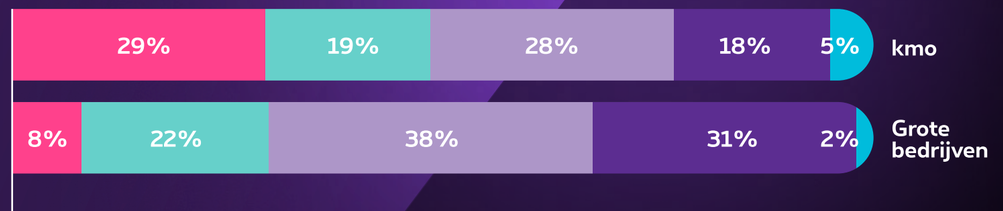
Cybersecuritybewustwording

Bewustwordingscampagnes leren medewerkers om dreigingen te herkennen en er adequaat op te reageren. Grote bedrijven verlenen de nodige opleidingen en voldoen op die manier aan de verwachte standaarden. Bij kmo's is er meer ruimte voor verbetering. Ze organiseren minder vaak trainingen op het gebied van cyberbeveiliging. Bijna een derde geeft aan dat nooit te doen. Nochtans begint weerbaarheid bij het bewustzijn van de medewerkers.



Hoe vaak organiseert uw bedrijf bewustmakingscampagnes op het gebied van cybersecurity (training, phishing-testmails, etc.)?

- Nooit
- Eenmaal per jaar
- Meerdere keren per jaar
- Voortdurend
- Ik weet het niet



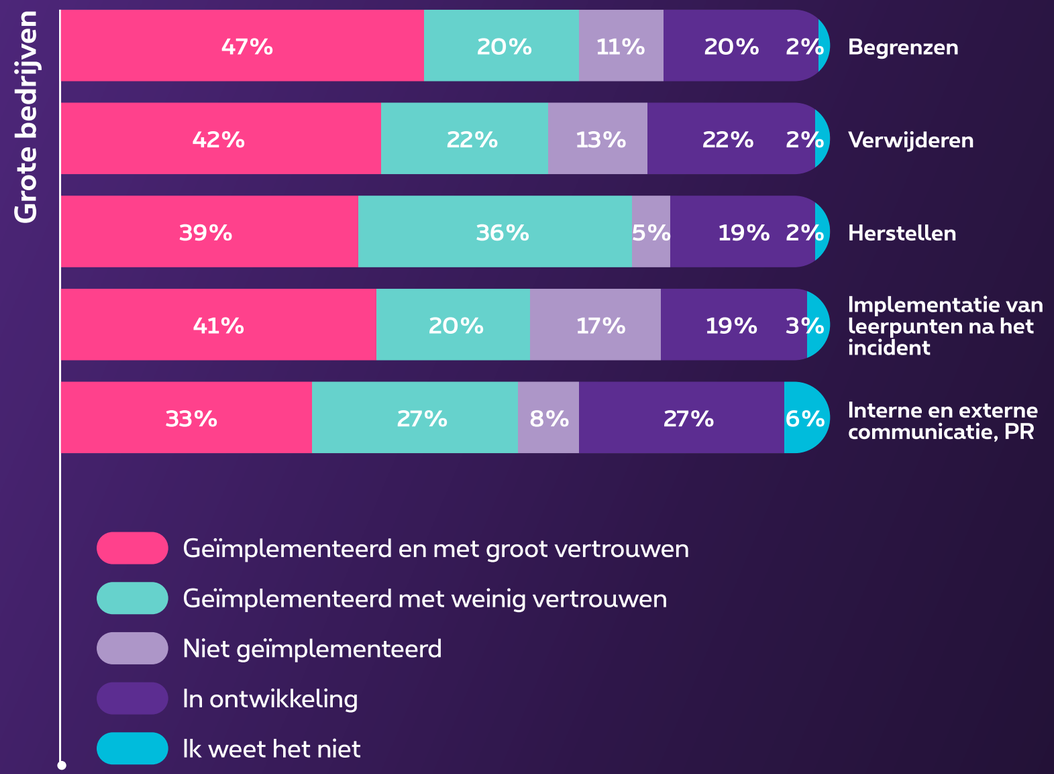
Hoe vaak organiseert uw bedrijf bewustmakingscampagnes op het gebied van cybersecurity (training, phishing-testmails, etc.)?

- Nooit
- Eenmaal per jaar
- Meerdere keren per jaar
- Voortdurend
- Ik weet het niet

Incident response process

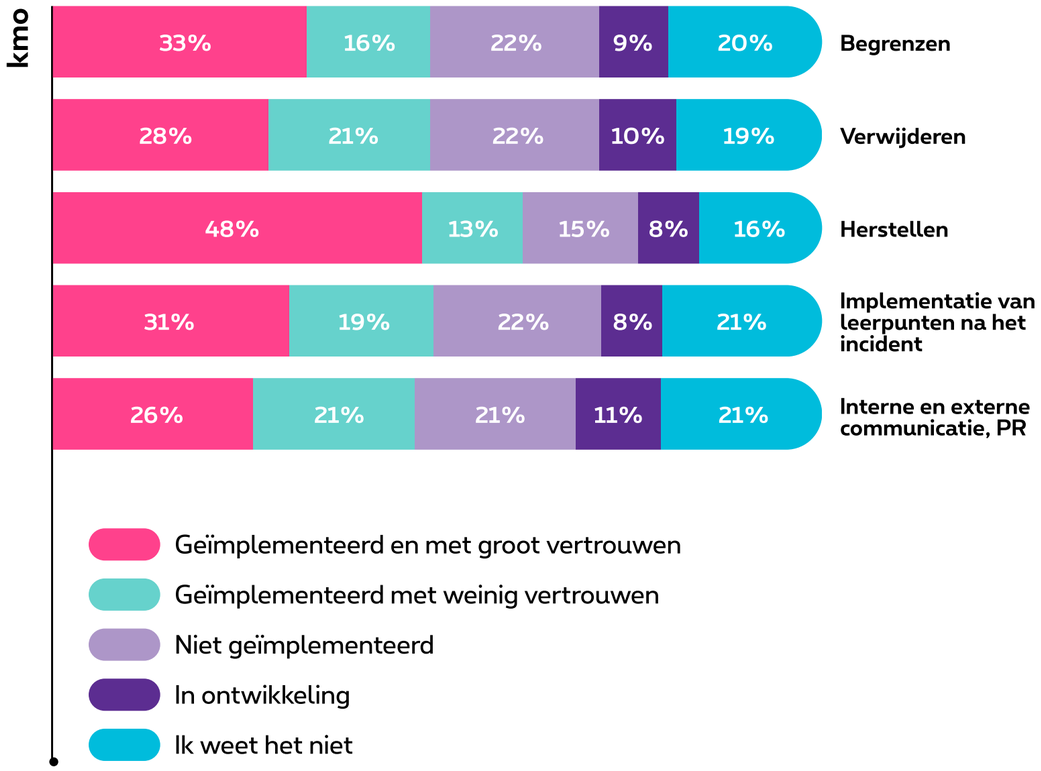
Een incident response process bundelt de instructies en processen om te reageren op incidenten en de veroorzaakte schade te herstellen. Grote ondernemingen tonen meer vertrouwen in hun opgezette structuren om risico's in te perken en aanvallen te bestrijden. Kleine en middelgrote organisaties tonen zich zekerder over hun herstelaanpak.

Beschikt uw bedrijf over een cybersecurity incident response process en hoeveel vertrouwen hebt u in uw capaciteiten voor incidentbeheer?



Beide groepen zien over de hele lijn nog lacunes binnen hun processen om incidenten efficiënt het hoofd te bieden. Interne en externe communicatie blijken - net als public relations - een werkpunt voor zowel kmo's als grote bedrijven. De feedback uit het onderzoek onderstreept het belang van een aanpak op maat. Terwijl grote ondernemingen voordeel halen uit hun schaal en middelen, kunnen kmo's hun flexibiliteit benutten om een robuuste herstelstrategie te ontwikkelen.

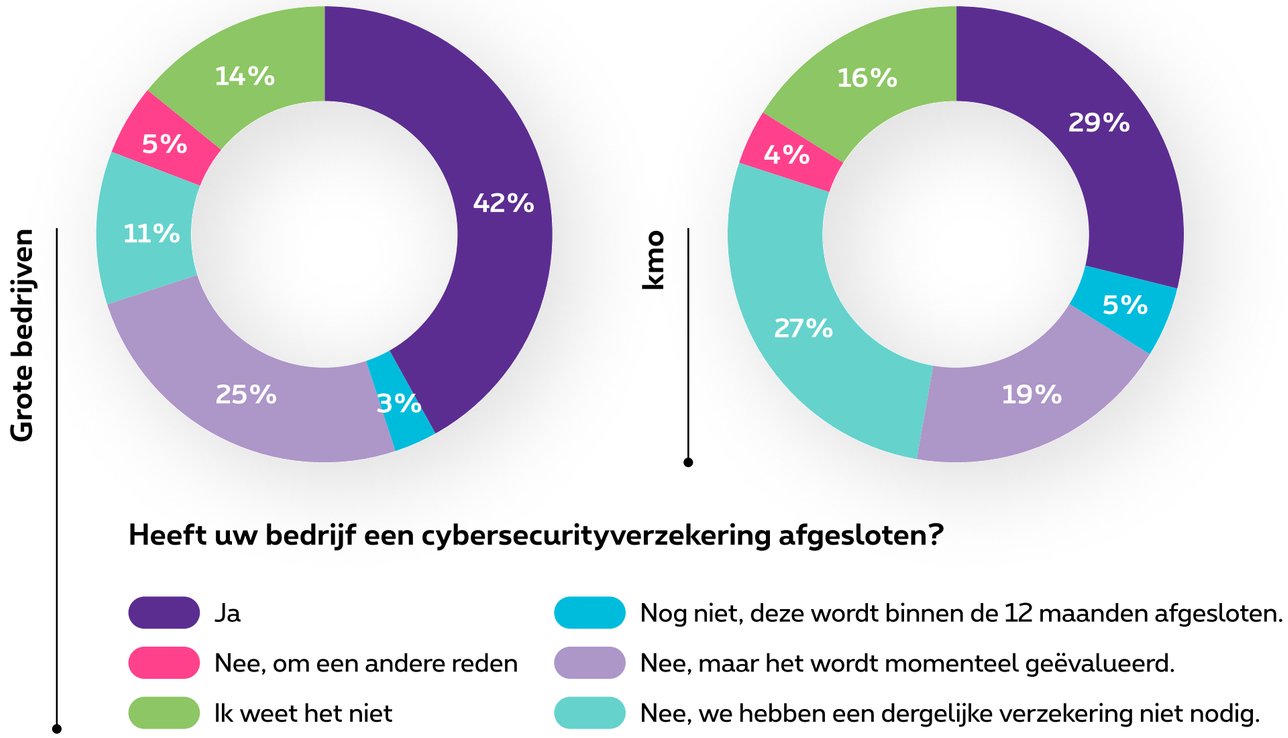
Beschikt uw bedrijf over een cybersecurity incident response process en hoeveel vertrouwen hebt u in uw capaciteiten voor incidentbeheer?



Cybersecurityverzekering

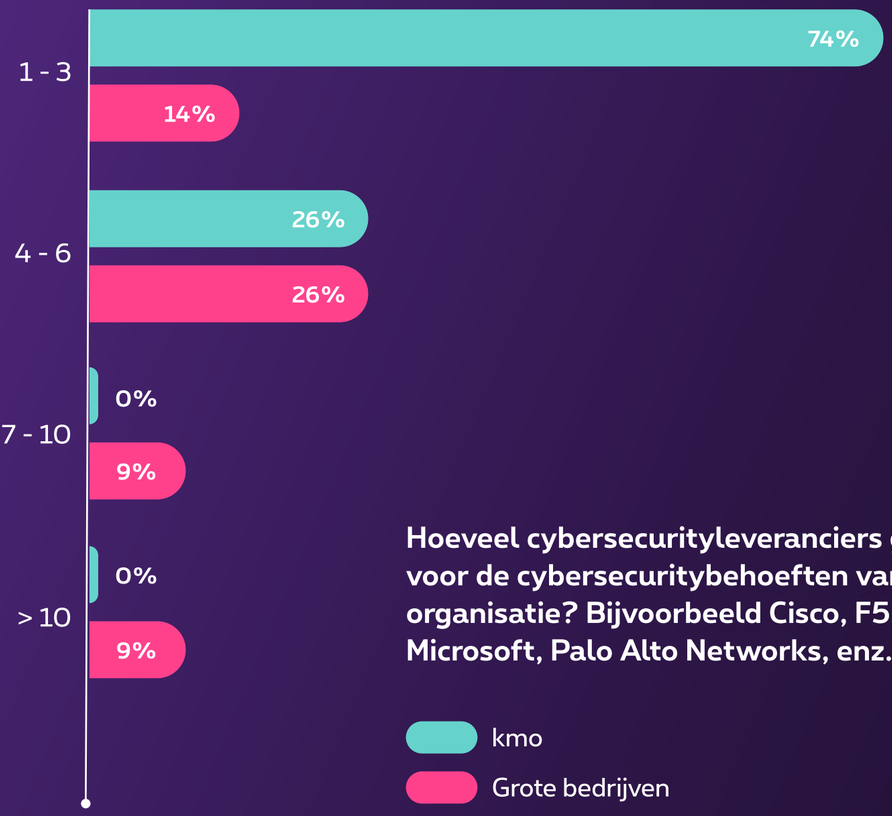
Onder invloed van een toenemend aantal dreigingen, grotere aangerichte schade en een strengere wetgeving verwacht Global Market Insight dat de cyberverzekeringsbranche tussen 2024 en 2032 jaarlijks zal groeien met 20,5%.

Ten opzichte van vorig jaar geven meer bedrijven aan dat ze een cybersecurityverzekering hebben afgesloten. Toch vinden veel kmo's zo'n polis nog altijd overbodig. Grotere organisaties zijn zich mogelijk meer bewust van de dreigingen en beschikken wellicht over meer middelen voor dergelijke verzekeringen, terwijl kmo's andere prioriteiten stellen en cyberbeveiligingsverzekeringen anders percipiëren.



Aantal technologie leveranciers

Uit het onderzoek blijkt dat de meeste kleine en middelgrote bedrijven de voorkeur geven aan een beperkt aantal cyberbeveiligingsleveranciers: bijna driekwart vertrouwt op slechts één tot drie leveranciers. Grotere organisaties laten een meer gespreide aanpak zien. Dat duidt op een trend naar eenvoud en mogelijk ook kostenefficiëntie bij kmo's, terwijl grotere ondernemingen het midden zoeken tussen diversiteit en beheerbaarheid.



Hoeveel cybersecurityleveranciers gebruikt u voor de cybersecuritybehoeften van uw organisatie? Bijvoorbeeld Cisco, F5, Fortinet, Microsoft, Palo Alto Networks, enz.

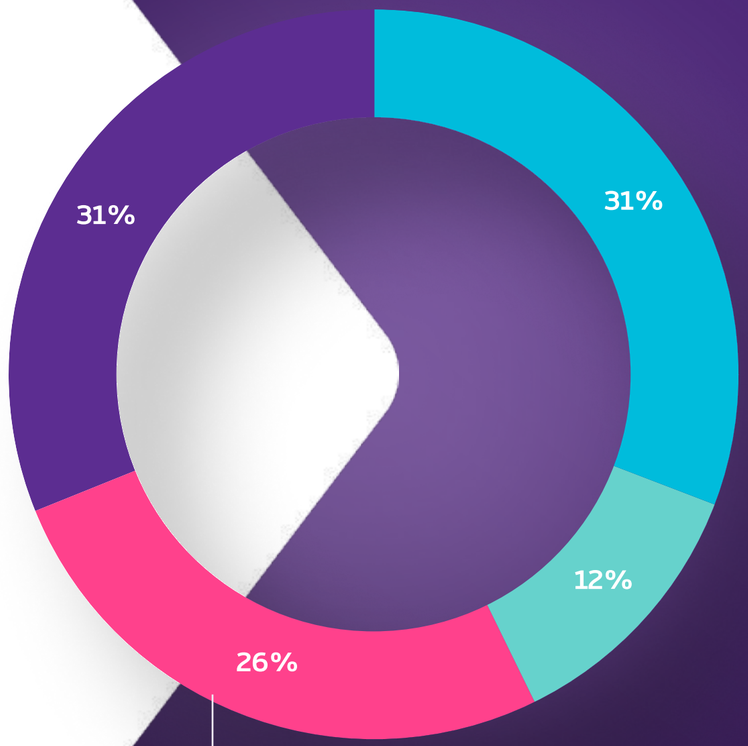
kmo

Grote bedrijven

Hoofdstuk 4

Onvoldoende NIS2 compliancy

De vraag om het beveiligingsbeleid verder aan te scherpen, komt er niet alleen uit eigen noodzaak. De NIS2-richtlijn biedt een uniform rechtskader om de cyberbeveiliging in de EU te handhaven. België zette als een van de eerste EU-lidstaten de NIS2-richtlijn om in nationale wetgeving. Luxemburg volgt binnenkort. Ondanks die urgentie weet 43% van de kmo's nog altijd niet of ze aan de NIS2-richtlijn moeten voldoen.



Valt uw organisatie onder de NIS2-richtlijn?

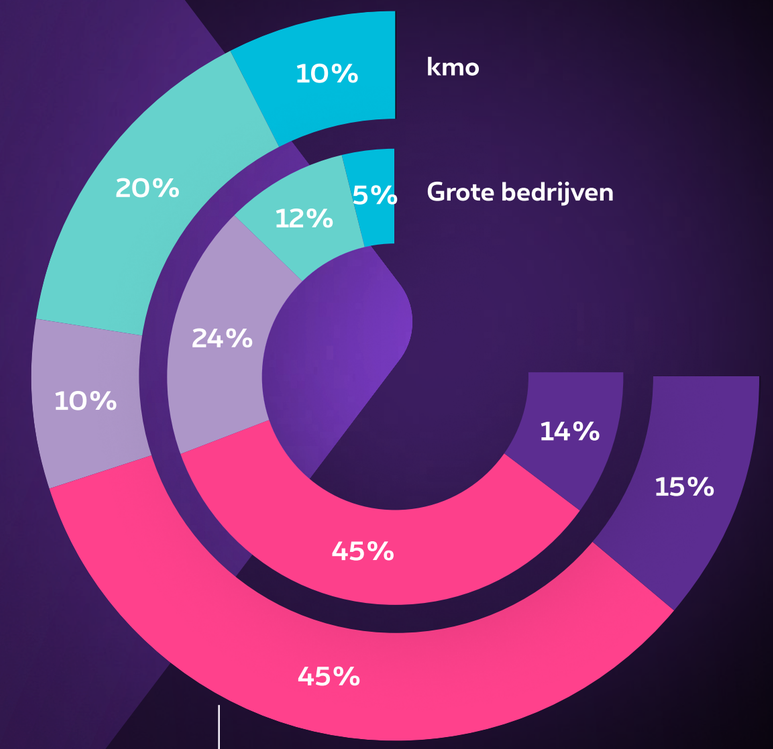
- Ja
- Ik denk van wel, maar weet het niet zeker
- Nee
- Ik weet het niet

Meer weten over NIS2?
Lees hier wat NIS2 betekent voor uw onderneming.

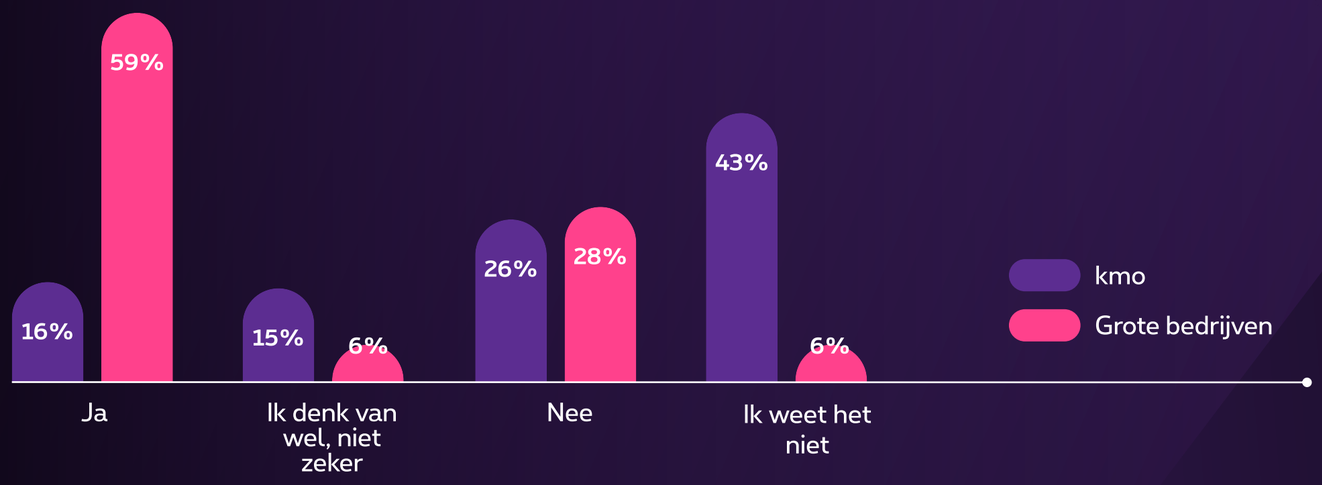
Kloof tussen richtlijn en realiteit

De resultaten van het onderzoek laten zien dat ongeveer 15% van de organisaties aangeeft volledig volgens de NIS2-richtlijn te handelen. Bedrijven die onzeker zijn over de kloof tussen de huidige en de benodigde maatregelen situeren zich vooral onder kmo's. Hetzelfde geldt voor de ondernemingen die het helemaal niet weten.

De resultaten van het onderzoek onderstrepen de voortdurende uitdaging om volledig in lijn met de NIS2-regelgeving te handelen. Dat geldt in het bijzonder voor grotere organisaties met complexere vereisten. Kleinere bedrijven, die zich op dat vlak in een betere positie lijken te bevinden, moeten waken over de beschikbare middelen en het nodige bewustzijn om aan de compliancenormen te voldoen.



Moet uw organisatie voldoen aan de nieuwe NIS2-regelgeving?



Is uw organisatie NIS2-conform?

- Ja, 100%
- Nee, maar wel meer dan 50%
- Nee, minder dan 50%
- Nee, onduidelijk hoeveel we al voldoen
- Ik weet het niet

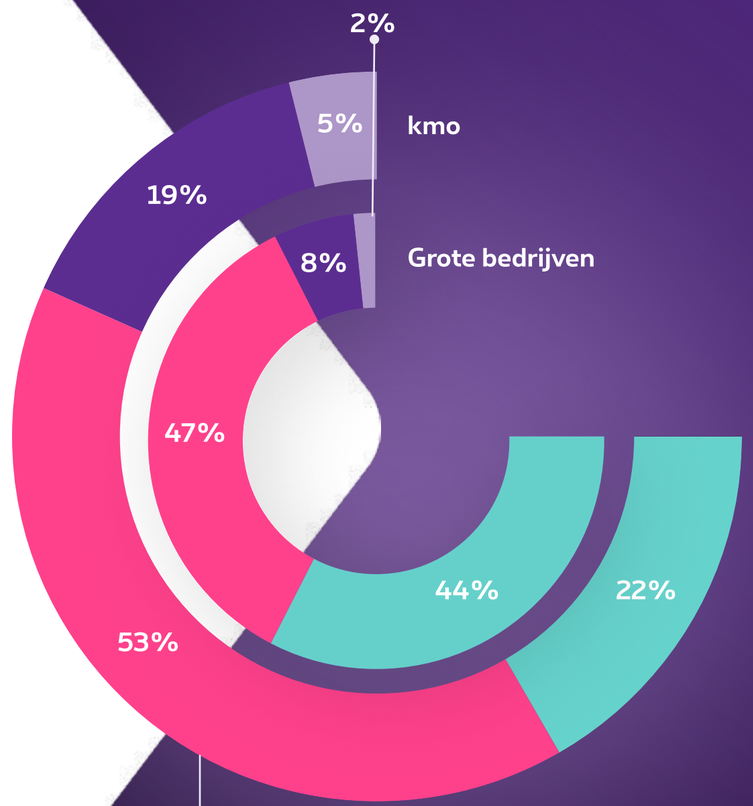
Hoofdstuk 5

Wat brengt de toekomst?

De opkomst van artificiële intelligentie en het groeiende aantal cloudapplicaties versnellen de digitale transformatie, maar creëren ook nieuwe aanvalsvlakken voor cybercriminelen. Zowel het aantal aanvallen als de complexiteit om die te bestrijden beloven allerminst af te nemen.

"Opvallend is dat veel bedrijven verwachten dat de tijd van zeer grote stijgingen van de cyberbeveiligings-budgetten achter de rug ligt, al blijft de meerderheid van de ondernemingen gewag maken van een stijging van de budgetten."

Wouter Vandenbussche,
Cybersecurity Services Lead bij Proximus NXT



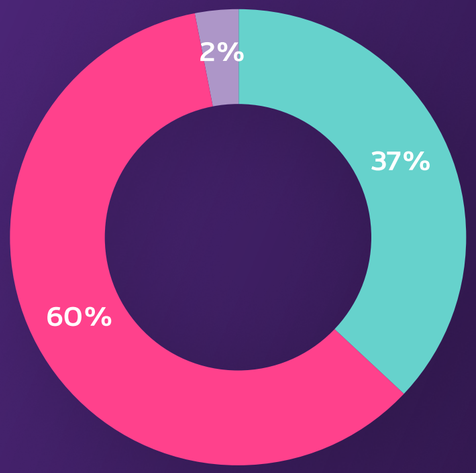
Hoe bezorgd bent u over de mogelijkheid dat u (opnieuw) wordt geconfronteerd met een cybersecurityincident?

- Zeer bezorgd
- Bezorgd
- Enigszins bezorgd
- Helemaal niet bezorgd

Blijvende dreiging

Het gros van de ondernemingen is zich bewust van het blijvende risico op cyberincidenten. Die bekommernis is het meest uitgesproken bij de grote bedrijven. Slechts een fractie van de bedrijven maakt zich vandaag minder zorgen om cyberveiligheid ten opzichte van een jaar geleden. De overgrote meerderheid is minstens even verontrust.

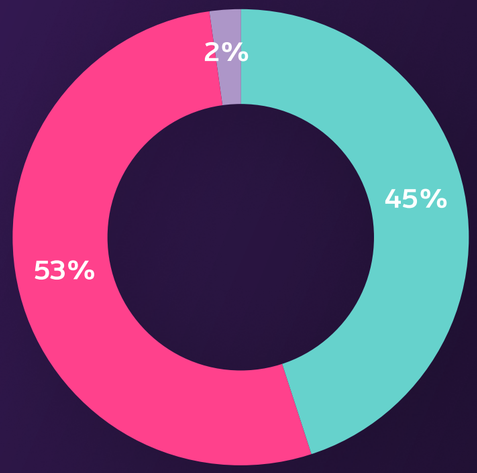
kmo



Hoe is uw bezorgdheid over het risico op een cyberincident geëvolueerd in de afgelopen 12 maanden?

- Bezorgdheid is toegenomen
- Bezorgdheid is hetzelfde gebleven
- Bezorgdheid is afgenomen

Grote bedrijven



Hoe is uw bezorgdheid over het risico op een cyberincident geëvolueerd in de afgelopen 12 maanden?

- Bezorgdheid is toegenomen
- Bezorgdheid is hetzelfde gebleven
- Bezorgdheid is afgenomen

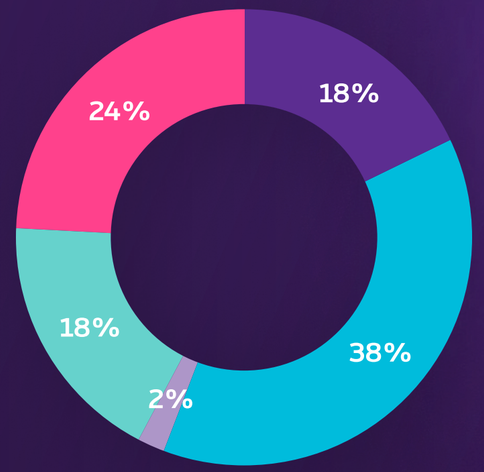
"Voor het derde opeenvolgende jaar verwacht meer dan 40% van de respondenten een toegenomen aantal cyberbeveiligingsincidenten of een grotere impact van dergelijke calamiteiten."

Wouter Vandenbussche,
Cybersecurity Services Lead
bij Proximus NXT

Securitydienstverleners

Hoewel de meeste kmo's en grote organisaties hun huidige cyberbeveiligingspartnerschappen willen behouden, is er ook een aanzienlijke interesse in het uitbreiden van die relaties.

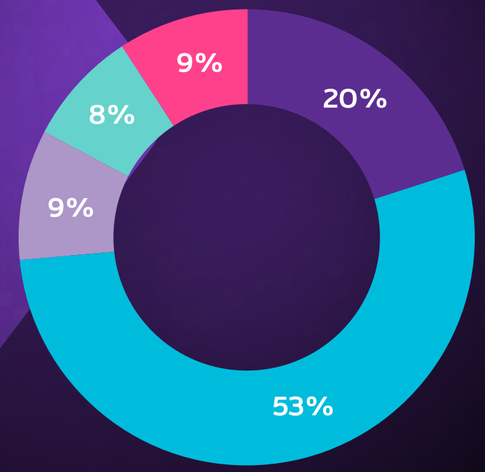
kmo



Hoe zal het aantal securitydienstverleners dat door uw organisatie wordt gebruikt evolueren de komende 12 maanden?

- Zal toenemen
- Zal min of meer hetzelfde blijven
- Zal afnemen
- Ik kan deze informatie niet vrijgeven
- Ik weet het niet

Grote bedrijven



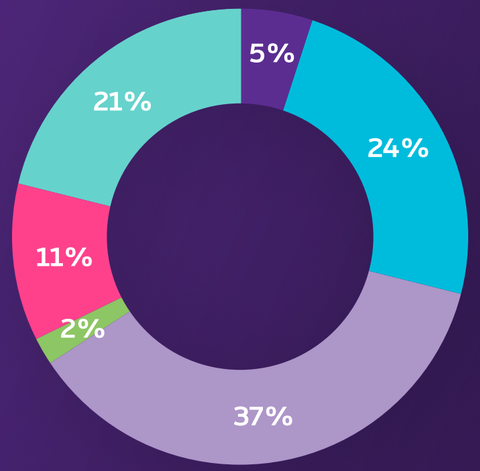
Hoe zal het aantal securitydienstverleners dat door uw organisatie wordt gebruikt evolueren de komende 12 maanden?

- Zal toenemen
- Zal min of meer hetzelfde blijven
- Zal afnemen
- Ik kan deze informatie niet vrijgeven
- Ik weet het niet

Budget

De meeste organisaties zijn van plan om hun budget voor cyberbeveiliging het komende jaar te verhogen of te handhaven. Grote bedrijven zijn meer geneigd om hun budget aanzienlijk op te trekken dan kleinere bedrijven. Slechts zeer weinig organisaties verwachten hun uitgaven voor cyberbeveiliging te verlagen, wat wijst op een algemene trend naar hogere investeringen.

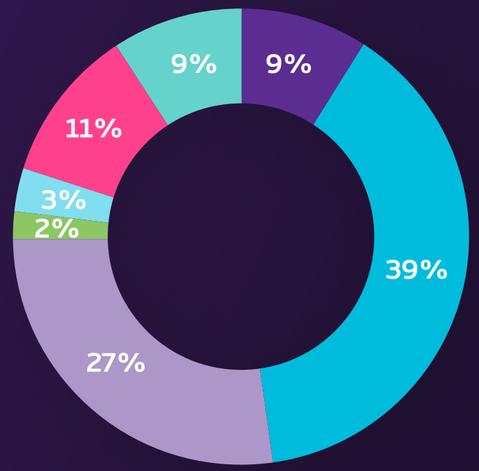
kmo



Hoe zal het cyberbeveiligingsbudget van uw organisatie de komende 12 maanden evolueren?

- Sterk stijgen (+ 20%)
- Stijgen (+ 1 to 19%)
- Blijft hetzelfde
- Afnemen (-1% to -9%)
- Sterk afnemen (-10%)
- Ik kan deze informatie niet vrijgeven
- Ik weet het niet

Grote bedrijven



Hoe zal het cyberbeveiligingsbudget van uw organisatie de komende 12 maanden evolueren?

- Sterk stijgen (+ 20%)
- Stijgen (+ 1 to 19%)
- Blijft hetzelfde
- Afnemen (-1% to -9%)
- Sterk afnemen (-10%)
- Ik kan deze informatie niet vrijgeven
- Ik weet het niet

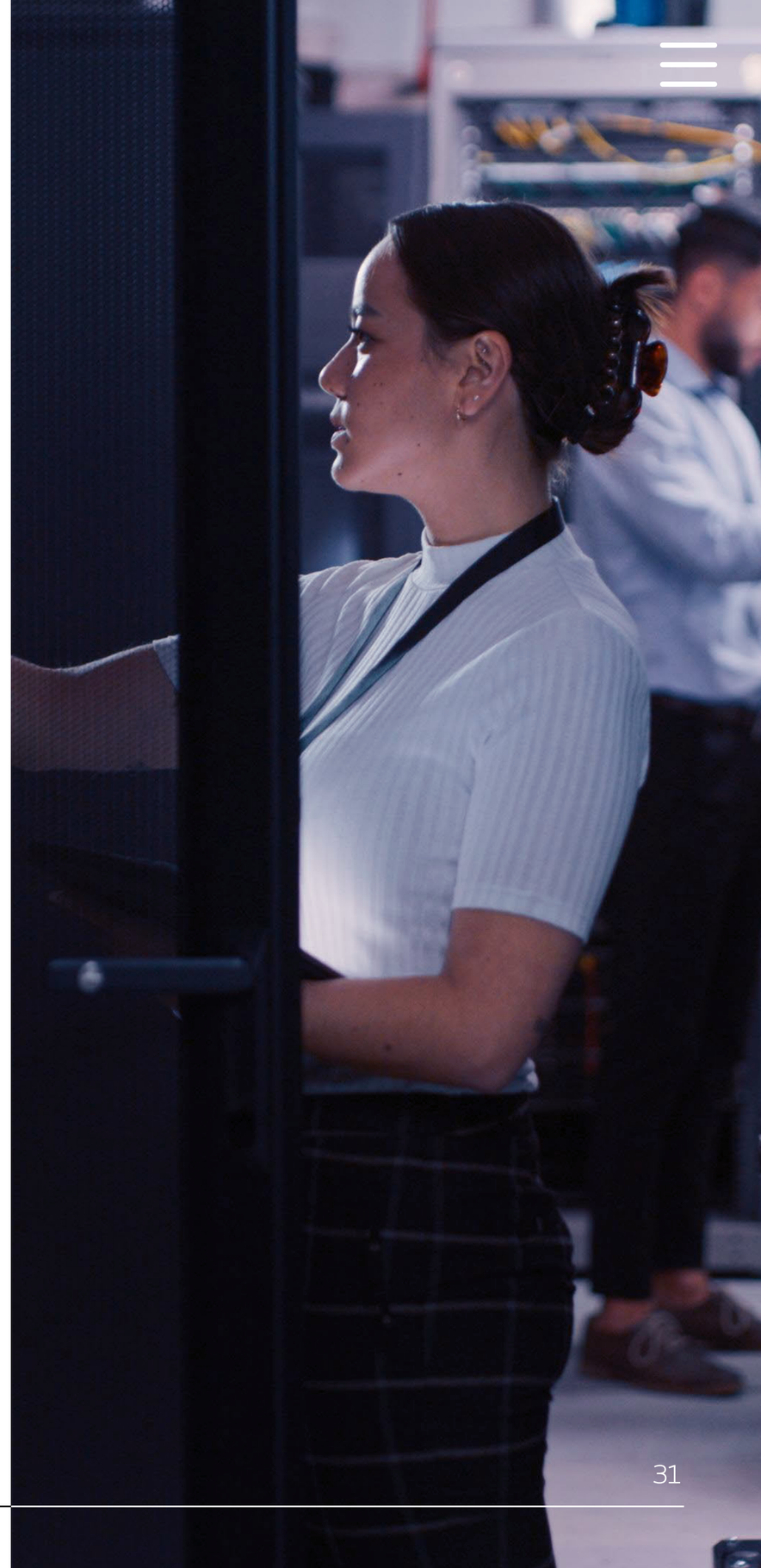
Toekomstige prioriteiten

Preventie blijft de topprioriteit voor de bevraagde organisaties, hoewel dat niet langer als enige aandachtsgebied naar voren komt. Binnen het domein van preventie vormt **identiteitsbescherming** een belangrijk aandachtspunt, grotendeels gedreven door het toepassen van een Zero Trust mindset als basis van de security architectuur.

Governance, Risk en Compliance (GRC) is een ander belangrijk aandachtspunt, waarbij bedrijven ernaar streven hun governance frameworks te versterken, risico's te beheren en de naleving van wettelijke vereisten te garanderen. Dat duidt op een groeiende bewustwording rond het belang van een robuust beleid, het voldoen aan de wettelijke normen en de nodige procedures om de cybersecurityrisico's te beperken.

Bewustwording en training treden als topprioriteit op de voorgrond, waarbij de nadruk ligt op de opleiding en training van werknemers rond best practices op het gebied van cyberbeveiliging. Die focus onderstreept het belang van een beveiligingsbewuste cultuur en de menselijke rol bij het voorkomen van incidenten.

Detectie en reactie gelden eveneens als prioriteiten, waarbij bedrijven hun capaciteiten vergroten om cyberbedreigingen te identificeren en erop te reageren.



Laten we connecteren

Beveilig uw netwerk en infrastructuur tegen geavanceerde aanvallen en voorkom dat de applicaties en websites van uw bedrijf onbereikbaar worden.

Ontdek de meest recente insights over cybersecurity

Praat met een expert over uw cybersecurity aanpak

proximus NXT