Cybersecurity-barometer

Cybersecurity-maturiteit bij Vlaamse bedrijven

situatie 2022

CYBERSECURITY VLAANDEREN
BOUWEN AAN JE DIGITALE TOEKOMST

Colofon

Cybersecurity-barometer – Cybersecurity-maturiteit bij Vlaamse bedrijven: situatie 2022 (Rapport ECOOM-STORE 22-030) is een publicatie in opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse overheid uitgevoerd door van ECOOM-STORE, UGent

Verantwoordelijke uitgever

Johan Hanssens, Secretaris-generaal

Vlaamse overheid, Departement Economie, Wetenschap en Innovatie (EWI)

Koning Albert II-laan 35, bus 10

1030 Brussel

Info.ewi@vlaanderen.be

Tel.: 02 553 59 80

Auteurs

Petra Andries, Cathy Lecocq en Thomas Standaert (ECOOM-STORE, UGent)

Tom Evens (Research Group for Media, Innovation & Technology, UGent)

Datum van uitgave

maart 2023

Depotnummer

D/2023/3241/107

DEPARTEMENT
ECONOMIE
WETENSCHAP &
INNOVATIE

Inhoudstafel

Samenvatting

In opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse overheid brengt deze CS-Barometer de maturiteit in cybersecurity (CS) bij Vlaamse bedrijven anno 2022 in kaart.

Deze CS-Barometer schetst een wetenschappelijk onderbouwd beeld van de mate waarin Vlaamse bedrijven CS-maatregelen in hun werking integreren en stoelt op **twee cruciale methodologische principes**. Ten eerste, een grootschalige, aselecte steekproef (steekproefaantal van 9.085 bedrijven, 2.367 bruikbare antwoorden in totaal) representatief voor de populatie van Vlaamse bedrijven volgens bedrijfsgrootte en sector van activiteit. Ten tweede, een gevalideerd meetinstrument in lijn met gelijkaardige Europese vragenlijsten.

De mate van CS-maturiteit van bedrijven wordt in belangrijke mate bepaald door een **combinatie van maatregelen**. Ten eerste, bedrijven kunnen *technische maatregelen* nemen, zoals toegangscontrole instellen of cryptografie gebruiken om bedrijfsgegevens te beschermen. Ten tweede, bedrijven kunnen verschillende *beheerprocedures* implementeren waarmee ICT- en operationele systemen worden gebruikt, beheerd en onderhouden. Ten derde, bedrijven kunnen maatregelen nemen om de *kennis en het bewustzijn* omtrent het beschermen van informatie, toestellen, systemen en netwerken bij het management en de medewerkers (alsook bij leveranciers) te verhogen. De CS-maturiteit van een bedrijf neemt toe naarmate het bedrijf op elk van deze aspecten maatregelen neemt.

In vergelijking met de voorgaande editie[1] van de CS-Barometer, omvat deze Barometer na overleg met de opdrachtgever twee additionele sectoren: (a) financiële activiteiten en verzekeringen en (b) menselijke gezondheidszorg en maatschappelijke dienstverlening. In dit rapport worden bijgevolg in hoofdzaak statistieken besproken die representatief zijn voor een populatie bestaande uit een breed scala van productie- en dienstensectoren. Om daarnaast een vergelijking met de voorgaande editie mogelijk te worden, werden bijkomend statistieken berekend waarbij de twee additionele sectoren buiten beschouwing werden gelaten.

[1] Andries, P., Evens, T., Maes, M., Reynaerts, J., Schuurman, D., & Georges, A. (2021). CS Barometer: Maturiteit in cybersecurity bij Vlaamse bedrijven https://steunpunt-economie-ondernemen.be/publicaties-1/c-ondernemen/store-21-003-b-cs-barometer-maturiteit-in-cybersecurity-bij-vlaamse-bedrijven

Globaal gezien zijn de **uitgaven voor CS door Vlaamse bedrijven het afgelopen jaar gestegen**. Vlaamse bedrijven spenderen gemiddeld 19,9% van het totale IT-budget aan cybersecurity. Voor de meerderheid (56,0%) bleef dit budget ongewijzigd, maar 41,2% van de bedrijven liet een – lichte of sterke – stijging noteren. **Bijna driekwart (71,8%) van de respondenten meent dat hun onderneming goed beschermd is tegen cyberaanvallen**.

Afgaand op de mate waarin Vlaamse bedrijven ook effectief inzetten op de adoptie en ontwikkeling van technische maatregelen, beheerprocedures, en beleidsdocumenten lijkt deze perceptie echter weinig gefundeerd en kunnen er nog heel wat stappen gezet worden om de cyberveiligheid te verbeteren:

- Hoewel de meerderheid van de Vlaamse bedrijven verschillende technische maatregelen neemt, blijven deze vaak beperkt tot relatieve basistoepassingen die een minder sterke bescherming bieden. **Slechts een minderheid wendt meer geavanceerde technische maatregelen aan.** Hierbij gaat het onder meer om maatregelen rond het bijhouden van log files om cyberaanvallen te analyseren (47,3%), periodieke ICT-veiligheidsanalyse (37,9%), ICT-veiligheidstesten (34,4%), of encryptietechnieken voor data, documenten of e-mails (30,0%). **Slechts een derde van de ondernemingen voorziet opleidingen of activiteiten rond cyberveiligheid voor medewerkers**. Zelfs vrij elementaire toepassingen, zoals regelmatige software-updates (91,5%), een systematisch beleid rond back-ups (89,5%), toegangsbeheer van het ondernemingsnetwerk (77,2%) en sterke paswoordauthenticatie (70,3%) worden niet door alle bedrijven toegepast.
- Daarnaast hebben bedrijven slechts een beperkt aantal beheerprocedures om zich tegen cyberrisico's te beschermen of om met actuele dreigingen om te gaan. Vlaamse bedrijven die technische maatregelen namen, implementeren vooral procedures om zich effectief te *beschermen* tegen cyberaanvallen (bijvoorbeeld toegangsbeheer of identificatiemanagement) (73,4%) en om van een cyberaanval te *herstellen* (zoals herstel van back-ups, her-installeren van systemen of wijzigen van wachtwoorden) (59,9%), maar zetten veel minder in op procedures om cyberaanvallen te *detecteren* (bijvoorbeeld continue monitoring van veiligheidsrisico's) (49,7%), gevoelige databronnen of kritieke bedrijfsprocessen die mogelijk doelwit zijn bij een mogelijke cyberaanval te *identificeren* (40,7%), en er adequaat op te *reageren* (bijvoorbeeld aan de hand van incidentanalyse of crisiscommunicatie) (37,0%). Slechts een kwart (23,6%) van de Vlaamse bedrijven die minstens één technische maatregel namen, heeft alle vijf procedures van het NIST-kader in zekere mate geïmplementeerd.

- Verder beschikt slechts 19,7% van de bedrijven die ten minste één technische maatregel treffen over een plan of beleidsdocument inzake cybersecurity, waarin mogelijke cyberrisico's voor het bedrijf worden gedefinieerd en een coherent geheel van acties en procedures worden vastgelegd.
- Slechts een kwart (27,3%) van de Vlaamse bedrijven legt eisen inzake cybersecurity op aan leveranciers of onderaannemers; een gelijkaardig aandeel (22,0%) van de bedrijven krijgt eisen opgelegd van klanten. Grote en middelgrote bedrijven leggen vaker eisen op én krijgen vaker eisen opgelegd.

We zien dat maar liefst 13,5% van de Vlaamse bedrijven het afgelopen jaar slachtoffer werd van een cyberaanval, waarbij cybercriminelen al dan niet met succes trachtten computersystemen onklaar te maken of persoonlijke of confidentiële gegevens te verkrijgen. **Dit aandeel is naar alle waarschijnlijkheid een onderschatting** aangezien (i) een cyberaanval onopgemerkt kan blijven, (ii) respondenten eerder geneigd zijn om zich een cyberaanval te herinneren en deze te rapporteren wanneer de cyberaanval uiteindelijk schade berokkende aan het bedrijf en/of (ii) bedrijven uit vrees voor reputatieschade terughoudend zijn om hierover te communiceren. **26,8% van de Vlaamse bedrijven is verzekerd tegen cyberaanvallen, maar zo'n verzekering neemt natuurlijk niet weg dat er heel wat schade wordt opgelopen. Het meest voorkomende operationele gevolg van een geslaagde cyberaanval is de onbruikbaarheid van ICT-systemen (28,7%).** Diefstal van bedrijfsgegevens (12,7%), vernietiging of corruptie van bedrijfsgegevens (7,8%), en onbruikbaarheid van operationele systemen (6,6%) zijn minder voorkomende operationele gevolgen. Naast operationele gevolgen kan een cyberaanval ook andere gevolgen hebben. **Zo kijkt de helft van de slachtoffers van een cyberaanval tegen extra kosten voor reparatie of herstel aan**. 14,1% lijdt inkomstenverlies door een cyberaanval. Minder frequent zijn reputatieschade (9,7%), verlies van leveranciers, partners of klanten (5,1%), betalen van losgeld (4,2%), en boetes van regulatoren (0,2%).

Er is dus zeker ook nood aan een goed overheidsbeleid dat bedrijven verder stimuleert en ondersteunt om hun cyberveiligheid te verbeteren. **11,4% van de Vlaamse bedrijven kent het *Vlaams Actieplan Cybersecurity*** dat in maart 2019 werd gelanceerd. Dit actieplan blijft belangrijk om bedrijven te sensibiliseren, te informeren, op te leiden en financieel te ondersteunen bij het duurzaam verbeteren van hun cyberveiligheid:

- **Een gebrek aan bewustzijn** bij de werknemers vormt voor 57,3% van de bedrijven een belangrijk obstakel bij de invoer en het gebruik van CS-maatregelen. Dit gebrek aan bewustzijn geldt bovendien zowel voor bedrijven met een lage adoptiegraad van

technische maatregelen (aantal genomen technische maatregelen kleiner dan of gelijk aan 5) als hoge adoptiegraad van technische maatregelen (aantal genomen technische maatregelen groter dan 5) en **belemmert hiermee de CS-maturiteit.** Het hoeft daarom niet te verbazen dat **44,0% van de Vlaamse bedrijven een gebrek aan bewustzijn als het grootste cyberrisico beschouwt**. Dit maakt het des te vreemder dat slechts een derde van de bedrijven relevante opleidingen voorziet (zie punt hierboven).

- Naast bewustwording vormt **het gebrek aan relevante kennis, vaardigheden en ervaring** een belangrijk obstakel bij de invoer en het gebruik van CS-maatregelen. In 58,9% van de bedrijven heerst een gebrek aan kennis, vaardigheden en ervaring. Bovendien ervaart 39,6% van de bedrijven moeilijkheden om werknemers met de vereiste kennis, vaardigheden en ervaring te selecteren en aan te werven.
- Bovendien vormt in ongeveer één op vier bedrijven de **visie van het management** nog een obstakel. Zo ziet men onvoldoende het nut in van cybersecurity en/of wordt er te weinig prioriteit aan gegeven.

Terwijl het overheidsbeleid dus zeker moet blijven inzetten op sensibilisering en versterking van de competenties bij de Vlaamse bedrijven, blijft het – vooral voor kmo's – ook belangrijk om waar nodig **beroep te doen op gespecialiseerde externe competenties**. Hoewel het merendeel (76,5%) van de Vlaamse bedrijven beroep doet op externe algemene IT-dienstverleners voor hun beveiligingsgerelateerde activiteiten, schakelt slechts 30,3% (daarnaast) externe gespecialiseerde CS-dienstverleners in. Cybersecurity is zo'n specifiek en snel evoluerend vakgebied dat een onderneming er niet kan van uitgaan dat alle aspecten worden beheerst door het eigen personeel en/of een algemene IT-dienstverlener. Samenwerking met en uitbesteding aan gespecialiseerde partijen is dus een belangrijke factor in het verbeteren van de cyberveiligheid bij ondernemingen in Vlaanderen. Van de Vlaamse bedrijven met een lage adoptiegraad van technische CS-maatregelen noemt ongeveer de helft een **gebrek aan kennispartners of begeleiding als obstakel**. Hier kan het Vlaams Actieplan Cybersecurity verder op inspelen.

Inleiding

Onze maatschappij digitaliseert en automatiseert in een snel tempo. Bedrijven maken in toenemende mate gebruik van industrie-4.0-technologieën zoals artificiële intelligentie (AI), robots of Internet of Things om hun concurrentiepositie te versterken. Tegelijkertijd vormt deze toenemende afhankelijkheid van digitale netwerkinfrastructuur een belangrijke bron van kwetsbaarheid en bedreiging. Een adequaat beleid inzake cybersecurity (CS) is van cruciaal belang

voor de digitale economie en beschermt bedrijven, overheden en andere organisaties tegen schadelijke cyberaanvallen en kwaadwillige inbreuken op operationele en computernetwerken. Het Vlaams Actieplan Cybersecurity versterkt het bestaande overheidsinstrumentarium om bedrijven te informeren, sensibiliseren, begeleiden én te ondersteunen in het gebruik van cybersecuritytoepassingen[2].

In opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse Overheid brengt voorliggende CS-Barometer de **adoptie van, het gebruik van en de expertise in CS bij Vlaamse bedrijven** in kaart. De bedoeling bestaat erin een actuele monitoring van de maturiteit, obstakels en noden inzake CS te verschaffen en zodanig de impact van het desbetreffende Vlaamse actieplan mee te helpen evalueren. Toekomstige meetmomenten bieden de mogelijkheid om een longitudinaal overzicht van de evolutie inzake CS bij Vlaamse bedrijven te verwerven.

Deze CS-Barometer schetst een wetenschappelijk onderbouwd beeld van de mate waarin Vlaamse bedrijven CS-maatregelen in hun werking en aanbod integreren. Om een accuraat beeld van de onderzochte problematiek te bekomen, stoelt deze CS-Barometer op twee cruciale methodologische principes:

(1) **Representativiteit:** een grootschalige, aselecte steekproef representatief voor de populatie van Vlaamse bedrijven volgens bedrijfsgrootte en sector van activiteit;
(2) **Vergelijkbaarheid:** een gevalideerd meetinstrument in lijn met gelijkaardige Europese vragenlijsten.

Bovenstaande principes zijn cruciaal om de vergelijkbaarheid met andere studies die de adoptiegraad van CS-maatregelen bij Vlaamse bedrijven in kaart brengen te evalueren. Indien deze studies niet stoelen op dezelfde methodologische principes inzake representativiteit en vergelijkbaarheid is er weinig tot geen wetenschappelijke grond om de resultaten van diverse studies met elkaar te vergelijken.

[2] Zie https://www.ewi-vlaanderen.be/nieuws/vlaamse-regering-hecht-goedkeuring-aan-onderzoeksprogramma-cybersecurity-initiative-flanders

Methodologie

Meetinstrument

Inzake meetinstrument werd, net als in de editie van 2021, een maximale vergelijkbaarheid met gelijkaardige Europese vragenlijsten en onderzoeksinitiatieven nagestreefd. De vragenlijst omvat module D (ICT-security) van de *2022 Survey on ICT Usage and E-Commerce in Enterprises* aangewend door Eurostat[3] en Statbel[4], en gepubliceerd in de Digital Economy and Society Index (DESI)[5]. Deze module werd aangevuld met bestaande elementen uit andere relevante nationale en internationale studies[6]. Tot slot werden nieuwe elementen inzake de impact van CS op de bedrijfsprestaties en de kennis over beleidsondersteunende maatregelen van de Vlaamse overheid opgenomen.

De ontwikkeling van een stabiel meetinstrument in lijn met de structurele dataverzamelingen van officiële instanties zoals Eurostat en Statbel biedt perspectieven voor het verzamelen van longitudinale gegevens over het gebruik van en expertise in CS bij Vlaamse bedrijven. Op basis van periodieke meetmomenten kan een evolutie ter zake worden geschetst.

Populatie, steekproeftrekking en contactinformatie

In overleg met de opdrachtgever werd vastgelegd welke economische sectoren en grootteklassen van bedrijven dienden opgenomen te worden in het onderzoek. Het gaat om bedrijven in een breed scala van productie- en dienstensectoren (zie Tabel 1 in Appendix voor een overzicht van de geselecteerde sectoren). Sectoren opgenomen in de CS-Barometer die de situatie anno 2021 in kaart bracht werden opnieuw opgenomen. Daarbovenop werden ook bedrijven actief in financiële activiteiten en verzekeringen (NACE 64-66) en menselijke gezondheidszorg en maatschappelijke dienstverlening (NACE 86-88) opgenomen. Zowel grote, middelgrote, kleine als micro-ondernemingen – gecategoriseerd in grootteklassen op basis van het werknemersaantal – werden opgenomen. Voor deze laatste grootteklasse werd weliswaar een ondergrens van minstens vijf werknemers gehanteerd.

[3] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_e_esms.htm
[4] https://statbel.fgov.be/en/themes/enterprises/ict-and-e-commerce-enterprises#documents
[5] https://digital-strategy.ec.europa.eu/en/policies/desi
[6] IPSOS (2022). Cyber Security Breaches Survey 2022 (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022); Coomans, P.; Callewaert, K.; Codenie, W. & Schellekens, Y. (2021). Cybersecurity in de maakindustrie (https://www.digitaletoekomst.be/sites/default/files/2021-04/studie_cybersecurity_maakindustrie_NL.pdf)

De Bel-first-databank van Bureau van Dijk werd als vertrekpunt gehanteerd voor de steekproef, die gestratificeerd werd naar economische sectoren en grootteklassen (zie Tabel 1 voor populatie- en steekproefaantallen, gestratificeerd naar sector en grootteklasse). Alle (i) bedrijven met maatschappelijke zetel in Vlaanderen en (ii) bedrijven met maatschappelijke zetel in Brussel én minstens één vestiging in Vlaanderen werden geselecteerd. Omwille van de hoge mate van ontbrekende waarden voor werknemersaantallen in Bel-first, raadpleegden we de RSZ databank om bedrijven onder te verdelen in grootteklassen.

In lijn met internationaal onderzoek werd een oververtegenwoordiging van middelgrote en grote bedrijven in de finale dataset beoogd. Dit had onmiddellijke implicaties voor de steekproeftrekking. In praktijk werden alle middelgrote en grote bedrijven (in de geselecteerde sectoren) bevraagd waarvoor contactinformatie werd gevonden. Van de micro- en kleine bedrijven in de populatie werd in totaal 16% geselecteerd (rekening houdend met de verdeling over de verschillende sectoren).

Voor elk bedrijf in de steekproef werd vervolgens een contactpersoon en bijhorend e-mailadres opgezocht. Dit gebeurde in de eerste plaats aan de hand van persoonsgegevens die naar aanleiding van de CS-Barometer editie 2021 verzameld werden. Deze werden aangevuld met gegevens uit Trends Top, en via manuele opzoekingen op internet en informatie in Bel-first wanneer de informatie uit Trends Top niet beschikbaar of onvolledig was.

Bij voorkeur identificeerden we voor elk bedrijf in de steekproef een contactpersoon voor wie (a) de functietitel wijst op verantwoordelijkheid voor technologische ontwikkelingen binnen het bedrijf en (b) een persoonlijk e-mailadres beschikbaar is[7]. Indien geen contactpersoon met deze functietitel werd gevonden, werd voor een contactpersoon met een meer algemene management- of IT-functie geopteerd. Indien voor een micro- of kleine onderneming geen persoonlijk e-mailadres werd gevonden, werd een algemeen e-mailadres ter attentie van de zaakvoerder geregistreerd. Middelgrote en grote ondernemingen waarvoor een contactpersoon maar géén persoonlijk emailadres gevonden werd, werden per brief gecontacteerd.
De totale steekproef bevatte 9.085 bedrijven, waarvan er 8.398 per e-mail en 687 per brief gecontacteerd werden. De dataverzamelingsperiode liep van juni tot september 2022.

[7] De keuze voor deze contactpersoon kan mogelijk verklaren waarom de statistieken in dit rapport afwijken van deze verzameld in andere, meer algemene bevragingen zoals deze door Eurostat en Statbel, die gericht zijn aan ICT-managers.

Respons en weging

Van de 8.398 bedrijven die we via e-mail contacteerden, konden we er 7.459 bereiken. 939 e-mails konden niet afgeleverd worden. Voor deze bedrijven werd nieuwe contactinformatie opgezocht, waardoor uiteindelijk 7.968 bedrijven werden bereikt. Van de 687 bedrijven die we per brief contacteerden, konden 3 brieven niet afgeleverd worden. In totaal konden we dus 8.652 bedrijven bereiken. Na het uitsturen van drie herinneringen per e-mail aan de bedrijven die via e-mail bereikt werden, en een doorgedreven telefonische opvolging van alle bedrijven in de steekproef, ontvingen we antwoorden van 2.908 bedrijven. Dit impliceert een responsgraad van 33,6% (2.908/8.652). Van deze antwoorden waren uiteindelijk 2.367 antwoorden bruikbaar (zie Tabel 2). 541 antwoorden vielen uit de responsgroep omdat (a) de vragenlijst werd ingevuld voor een ander ondernemingsnummer dan gevraagd, (b) we voor eenzelfde bedrijf twee antwoorden verkregen, of (c) geen enkele vraag betreffende cybersecurity werd beantwoord.

326 van de 2.367 bedrijven met een bruikbaar antwoord werden eind oktober 2022 opnieuw gecontacteerd om onduidelijkheden of inconsistenties in hun antwoord uit te klaren. De responsgraad voor deze bevraging met het oog op validatie bedroeg 71,2% (232/326). Deze respons liet ook toe regels op te stellen voor het oplossen van de inconsistenties voor de 94 bedrijven die niet antwoordden op onze vraag naar verduidelijking.

De mate waarin antwoorden op individuele vragen ontbraken lag binnen aanvaardbare grenzen. Ontbrekende gegevens werden bij voorkeur geïmputeerd op basis van logische regels. Indien deze imputatiemethode niet mogelijk was, werden de ontbrekende gegevens geïmputeerd door middel van de *random-hot-deck* imputatiemethode.

Voor elk bedrijf dat antwoordde, werd nagegaan tot welk stratum het behoorde. Het kreeg vervolgens een gewicht, afhankelijk van het totaal aantal bedrijven in de populatie voor dat stratum en van het totaal aantal bruikbare antwoorden voor dat stratum. Dit rapport presenteert dan ook gewogen statistieken, die – omwille van deze weging – representatief zijn voor de totale bedrijfspopulatie beoogd in het onderzoek.

Tabel 1: Populatie- en steekproefaantallen per stratum (steekproefaantallen schuin gedrukt)

	NACE 10-33 (maakindustrie)	NACE 35-39 (nutssector)	NACE 41-43 (bouwnijverheid)	NACE 45-47 (groothandel en detailhandel; reparatie van auto's en motorfietsen)	NACE 49-53 (vervoer en opslag)	NACE 55-56 (accommodatie en maaltijden)	NACE 58-63 (informatie en communicatie)	NACE 64-66 (financiële activiteiten en verzekeringen)	NACE 68-75 (onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten)	NACE 77-82;95.1 (administratieve en ondersteunende diensten; reparatie van computers en communicatie-apparatuur)	NACE 86-88 (menselijke gezondheids - zorg en maatschappelijke dienstverlening)	**Totaal**
Micro (5-9 werknemers)	1.584	82	2.582	4.377	952	1.516	621	745	2.124	902	484	15.969
	251	13	411	693	148	243	99	118	338	143	77	2.534
Klein (10-49 werknemers)	2.471	161	2.417	4.698	1.409	844	809	438	1.745	1.002	760	16.754
	394	25	385	748	221	135	127	70	279	159	122	2.665
Middelgroot (50-249 werknemers)	826	41	323	669	328	48	172	82	291	397	598	3.775
	753	36	284	535	282	32	145	57	240	277	470	3.111
Groot (>= 250 werknemers)	217	21	48	143	57	18	29	24	73	132	191	953
	196	19	42	109	46	13	26	18	57	106	143	775
Totaal	5.098	305	5.370	9.887	2.746	2.426	1.631	1.289	4.233	2.433	2.033	37.451
	1.594	93	1.122	2.085	697	423	397	263	914	685	812	9.085

Tabel 2: Respons per stratum

	NACE 10-33 (maakindustrie)	NACE 35-39 (nutssector)	NACE 41-43 (bouwnijverheid)	NACE 45-47 (groothandel en detailhandel; reparatie van auto's en motorfietsen)	NACE 49-53 (vervoer en opslag)	NACE 55-56 (accommodatie en maaltijden)	NACE 58-63 (informatie en communicatie)	NACE 64-66 (financiële activiteiten en verzekeringen)	NACE 68-75 (onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten)	NACE 77-82;95.1 (administratieve en ondersteunende diensten; reparatie van computers en communicatieapparatuur)	NACE 86-88 (menselijke gezondheidszorg en maatschappelijke dienstverlening)	**Totaal**
Micro (5-9 werknemers)	63	2	92	163	32	36	44	25	91	34	20	602
Klein (10-49 werknemers)	92	8	92	197	48	25	41	16	76	37	33	665
Middelgroot (50-249 werknemers)	237	12	61	121	63	8	51	17	68	60	152	850
Groot (>= 250 werknemers)	64	8	15	26	16	2	7	3	17	32	60	250
Totaal	456	30	260	507	159	71	143	61	252	163	265	2.367

Resultaten

Dit onderdeel behandelt het bewustzijn en de aanpak van cybersecurity (CS) bij Vlaamse bedrijven. CS verwijst naar het beschermen van computers, servers, netwerken, mobiele toestellen, software, elektronische systemen en data tegen schadelijke cyberaanvallen. Een cyberaanval is een kwaadwillige inbreuk op de veiligheidssystemen van een onderneming met als motief operationele of computersystemen onklaar te maken, persoonlijke of confidentiële gegevens te los te weken of een losgeldbetaling te verkrijgen. Cyberaanvallen zijn er in diverse gradaties, gaande van phishing (frauduleuze berichten) of malware (kwaadaardige software), tot hacking en DDoS (distributed denial-of-service) waarbij netwerksystemen worden geïnfiltreerd of zelfs vergrendeld.

De mate van maturiteit van bedrijven inzake cybersecurity wordt in belangrijke mate bepaald door een combinatie van maatregelen. Ten eerste, bedrijven kunnen *technische maatregelen* nemen, zoals toegangscontrole instellen of cryptografie gebruiken om informatie te beschermen. Ten tweede, bedrijven kunnen *beheerprocedures* implementeren waarmee digitale systemen

worden gebruikt, bestuurd en onderhouden. Een adequaat CS-beleid is er op gericht cyberrisico's te beperken en de impact van eventuele incidenten zo klein mogelijk te houden. Dit is mogelijk door te beschikken over een set van procedures die op continue basis de risico's identificeren, gegevens en systemen beschermen, cyberaanvallen detecteren en waar nodig beantwoorden, én de situatie opnieuw herstellen. Naast de noodzakelijke technische maatregelen en beheerprocedures vormen medewerkers een derde belangrijke, en misschien zelfs meest kwetsbare, schakel in de bescherming van bedrijven tegen cyberaanvallen. *Kennis, vaardigheden en bewustzijn* omtrent het beschermen van informatie, toestellen en netwerken bij zowel het management als de medewerkers zijn immers essentieel voor de effectiviteit van technische maatregelen en beheerprocedures. De CS-maturiteit van een bedrijf neemt toe naarmate het bedrijf op elk van deze drie domeinen maatregelen neemt.

Perceptie bescherming en risico's

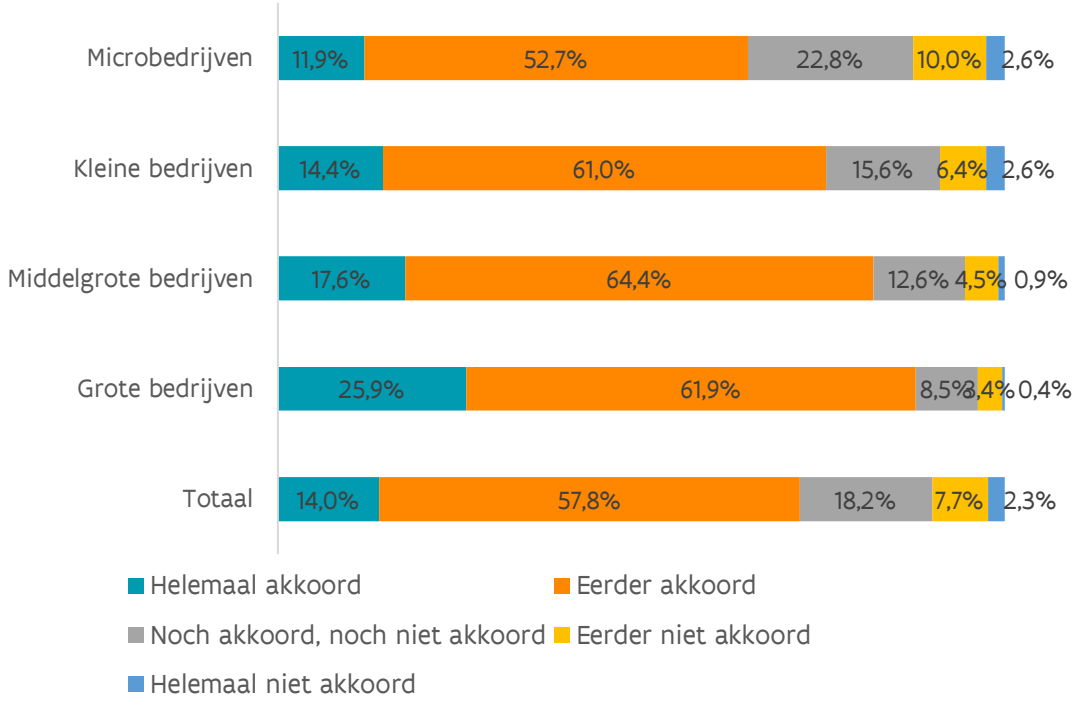
Vooraleer de maturiteit van bedrijven inzake cybersecurity in kaart te brengen aan de hand van objectieve maatstaven, werden respondenten gevraagd naar hun perceptie over (a) de mate van bescherming van hun onderneming tegen cyberaanvallen en (b) het grootste cyberrisico voor hun onderneming. Bijna driekwart (71,8%) van de respondenten is helemaal akkoord of eerder akkoord met de stelling dat hun onderneming goed beschermd is tegen cyberaanvallen (zie Figuur 1).

Deze score is beduidend hoger voor grote (87,8%) en middelgrote (82,0%) bedrijven dan voor kleinere ondernemingen. Ongeveer 90% van de bedrijven actief in financiële activiteiten en verzekeringen (NACE 64-66) en informatie en communicatie (NACE 58-63) is helemaal of eerder akkoord met de stelling, in tegenstelling tot minder dan de helft (47,3%) van de bedrijven in accommodatie en maaltijden (NACE 55-56).

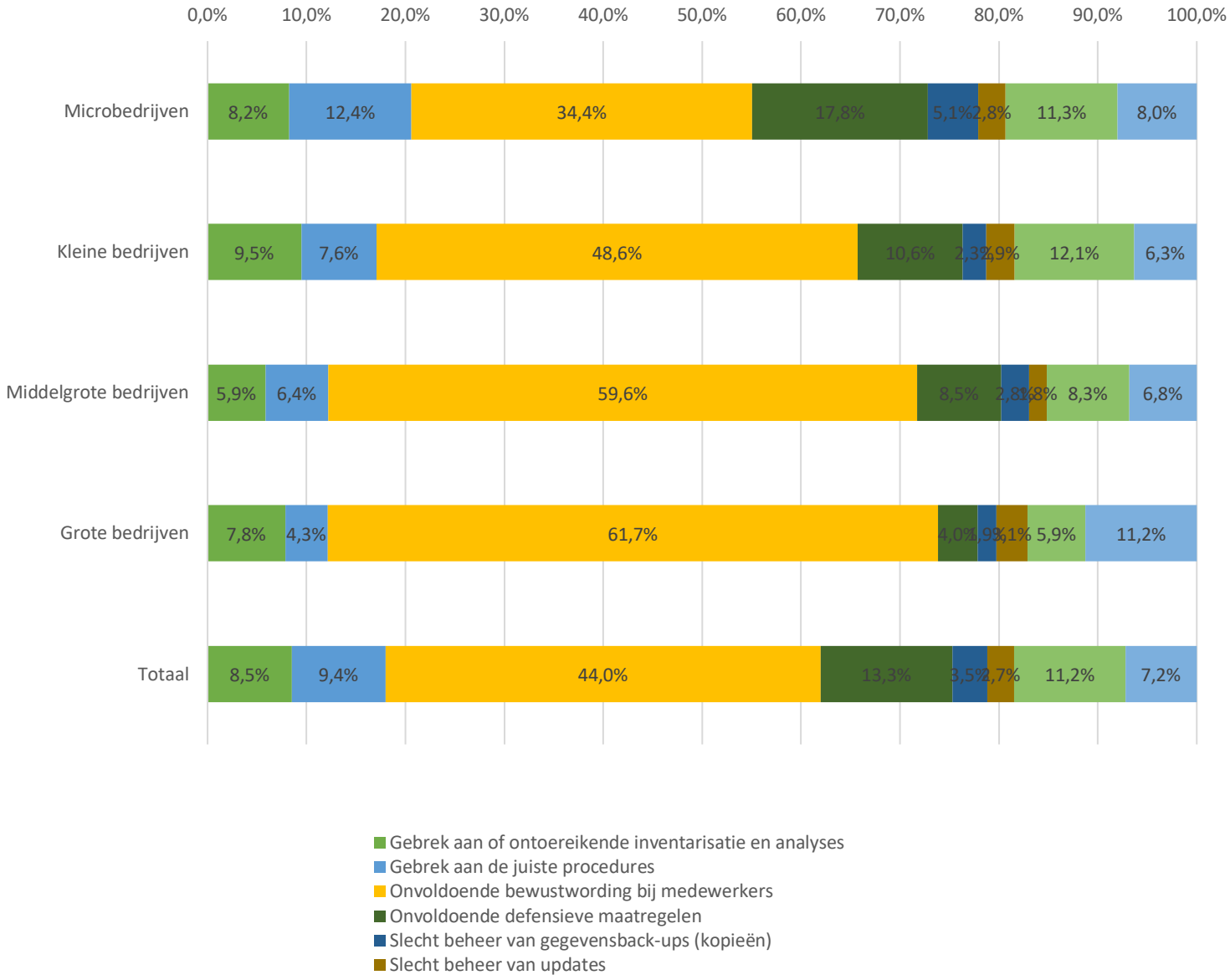
Volgens ongeveer de helft (44,0%) van de respondenten vormt onvoldoende bewustwording bij medewerkers het grootste cyberrisico voor hun onderneming (zie Figuur 2). Op ruime afstand volgen onvoldoende defensieve maatregelen (13,3%), gebrek aan (interne of externe) audits of evaluatie (11,2%), en gebrek aan de juiste procedures (9,4%). Slecht beheer van gegevensback-ups (3,5%) en slecht beheer van updates (2,7%) worden zelden als het grootste cyberrisico beschouwd. Onvoldoende bewustwording bij medewerkers wordt door grote (61,7%) en middelgrote (59,6%) bedrijven vaker als het grootste cyberrisico beschouwd (in vergelijking met kleinere bedrijven). Hoe kleiner het bedrijf, hoe vaker een gebrek aan defensieve maatregelen of juiste procedures als grootste cyberrisico wordt genoemd.

Bedrijven actief in informatie en communicatie (NACE 58-63), en onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (NACE 68-75) beschouwen een gebrek aan (interne of externe) audits of evaluaties vaker als grootste cyberrisico; bedrijven actief in de maakindustrie (NACE 10-33), bouwnijverheid (NACE 41-43), en accommodatie en maaltijden (NACE 55-56) beschouwen dan weer vaker onvoldoende defensieve maatregelen als het grootste cyberrisico.

Figuur 1: Mate waarin respondent akkoord gaat met de stelling "Onze onderneming is goed beschermd tegen cyberaanvallen" volgens bedrijfsgrootte (N=2.367)



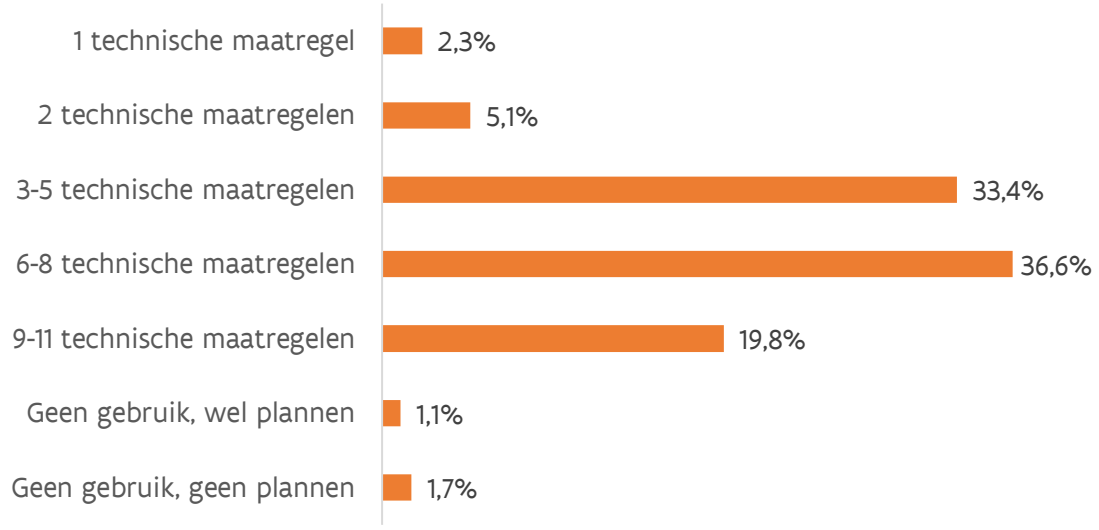
Figuur 2: Grootste cyberrisico volgens bedrijfsgrootte (N=2.367)



Technische maatregelen

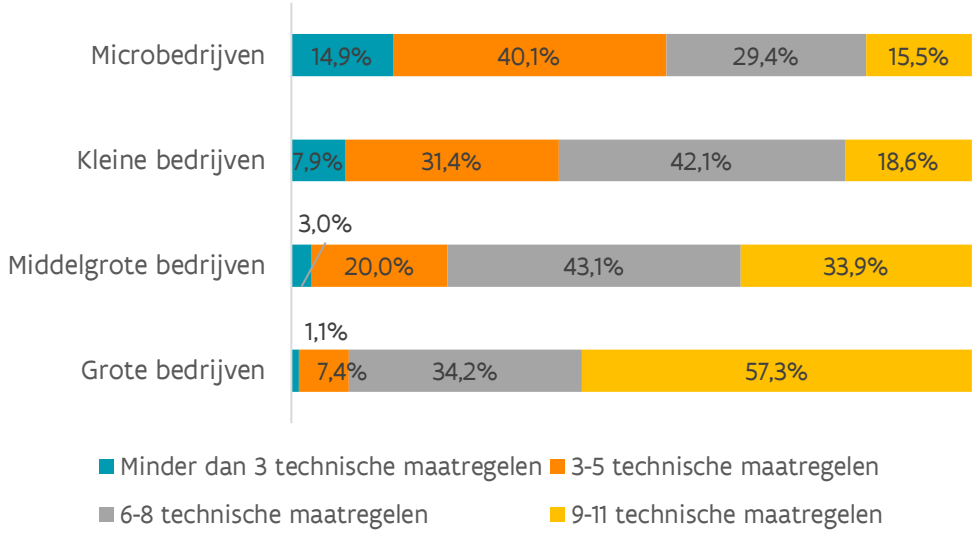
Naast de perceptie, bracht het onderzoek ook in kaart welke maatregelen bedrijven in Vlaanderen effectief nemen om zichzelf te beschermen tegen cyberaanvallen. De resultaten uit Figuur 3 geven aan dat de meerderheid van de Vlaamse bedrijven een veelheid aan technische maatregelen inzet om zijn cyberveiligheid zo goed als mogelijk te verzekeren. Na het voorleggen van een lijst van elf mogelijke technische maatregelen (zie verderop) zegt 33,4% van de bedrijven drie tot vijf technische maatregelen toe te passen. 36,6% past zes tot acht technische maatregelen toe, terwijl één op vijf (19,8%) bedrijven negen of meer van de bevraagde technische maatregelen toepast. In totaliteit past dus 97,2% van de Vlaamse bedrijven ten minste één technische maatregel toe. Dit wijst erop dat slechts een kleine minderheid (2,8%) geen enkele technische maatregel toepast in de dagelijkse werking. 1,7% van de bedrijven zegt geen plannen te hebben om één of meerdere technische maatregelen te implementeren in het komende jaar; 1,1% heeft daartoe wel plannen.

Figuur 3: Adoptiegraad aantal technische maatregelen (N=2.367)



Wanneer de bedrijfsgrootte (in termen van aantal werknemers) in beschouwing wordt genomen, is er een duidelijk verband met het aantal geïmplementeerde technische maatregelen: hoe groter een bedrijf, hoe meer technische maatregelen het bedrijf neemt (zie Figuur 4). 57,3% van de grote bedrijven past meer dan negen van de vooropgestelde technische maatregelen toe, een bijkomende 34,2% neemt zes tot acht technische maatregelen. Bij de middelgrote bedrijven bedraagt het aantal organisaties met negen of meer technische maatregelen 33,9%. Dit aantal ligt beduidend lager bij kleine bedrijven (18,6%) en microbedrijven (15,5%). Van deze laatste geeft 14,9% aan minder dan drie technische maatregelen te nemen.

Figuur 4: Adoptiegraad aantal technische maatregelen volgens bedrijfsgrootte (N=2.367)



Bedrijven kunnen een breed spectrum aan technische maatregelen nemen om een hogere cyberveiligheid te bekomen. Deze maatregelen gaan van eerder basis (zoals paswoordauthenticatie of software-updates) tot vrij geavanceerd (bijvoorbeeld biometrische authenticatie of encryptietechnieken).[8] Al naargelang de complexiteit vertoont de adoptie van deze technische maatregelen sterke verschillen (zie Figuur 5). Het regelmatig doorvoeren van software-updates, te beschouwen als een basismaatregel, wordt het meest toegepast (91,5%). Een bijna even vaak toegepaste maatregel is het maken van een data back-up naar een aparte locatie of in de cloud: 89,5% van de bedrijven geeft aan dit te doen. 77,2% heeft een protocol voor toegangsbeheer tot het ondernemingsnetwerk voor toestellen of gebruikers. Ook een sterke paswoordauthenticatie is met 70,3% stevig verankerd in de bedrijfswerking. Daarnaast beschikt ongeveer twee derde (66,6%) van de bedrijven over een VPN-netwerk.

Een minderheid van bedrijven neemt andere, vaak meer geavanceerde, technische maatregelen. Concreet gaat het hierbij om maatregelen rond het bijhouden van log files om cyberaanvallen te analyseren (47,3%), periodieke ICT-veiligheidsanalyse (37,9%) of ICT-veiligheidstesten (34,4%). Een minderheid van 30,0% past encryptietechnieken toe op data, documenten en/of e-mails; 18,7% gebruikt biometrische technieken ter identificatie en authenticatie van gebruikers (vingerafdrukken, stem- en/of gezichtsherkenning). Bovendien biedt slechts 34,2% van de Vlaamse bedrijven zijn werknemers opleidingen of activiteiten aan om hen bewust te maken van het belang van cybersecurity.

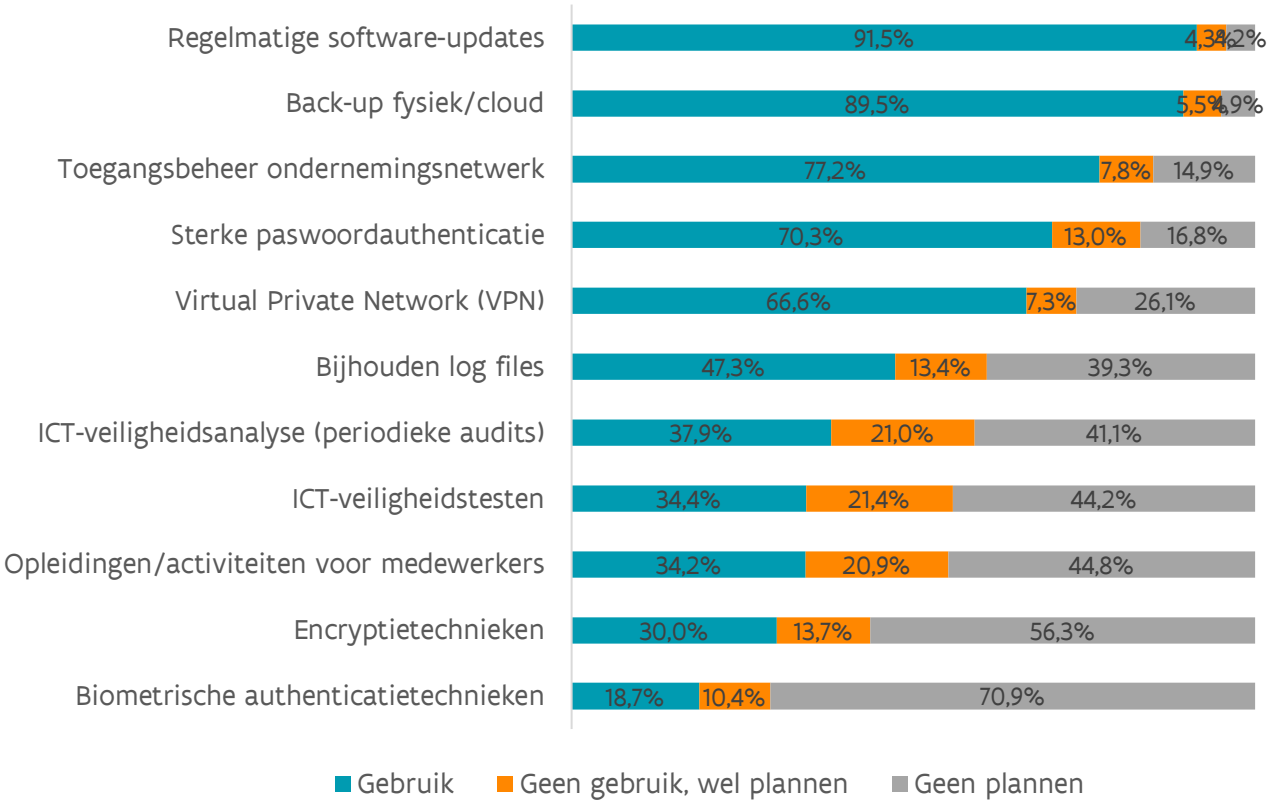
Vergeleken met de meting in 2021 is de adoptiegraad van minder geavanceerde technische maatregelen ofwel licht gestegen (data back-ups, VPN-netwerk, protocol voor toegangsbeheer, paswoordauthenticatie), ofwel vrijwel onveranderd gebleven (software-updates) (zie Figuur 23 in Appendix). Voor de meer geavanceerde technische maatregelen is de adoptiegraad ofwel grotendeels onveranderd gebleven (log files om cyberaanvallen te analyseren en (biometrische) encryptietechnieken), ofwel gedaald (periode ICT-veiligheidsanalyse en ICT-veiligheidstesten). De meest uitgesproken daling valt echter op te merken bij de adoptiegraad van opleidingen of activiteiten voor werknemers.

Bij de interpretatie van deze resultaten moet men er zich van bewust zijn dat een hoge adoptiegraad van deze of gene technische maatregelen niet noodzakelijk samengaat met een hoge

[8] Ongeacht de mate van complexiteit is de effectiviteit van een specifieke technische maatregel afhankelijk van de manier waarop deze geïmplementeerd wordt. Zo zijn bijvoorbeeld data back-ups naar een aparte locatie of in de cloud weinig doeltreffend indien deze niet op regelmatige basis gemaakt worden.

mate van CS-maturiteit. De meest optimale bescherming tegen cyberaanvallen ligt onder meer in de combinatie van een zo groot aantal van basis- én meer geavanceerde technische maatregelen. Het loutere feit dat bedrijven een aantal technische maatregelen treffen is in die optiek niet automatisch voldoende; de kracht van bescherming ligt immers in de combinatie van technische maatregelen. Bovendien wijzen de resultaten er op dat zelfs vrij elementaire basistoepassingen, zoals regelmatige software-updates, sterke paswoordauthenticatie, toegangsbeheer van het ondernemingsnetwerk en een systematisch beleid rond back-ups niet door alle bedrijven worden toegepast. Het is ook belangrijk er op te wijzen dat slechts een minderheid van bedrijven opleidingen of activiteiten aanbiedt om het bewustzijn en de kennis van zijn medewerkers omtrent cybersecurity te verhogen. Dit is des te meer opvallend omdat onvoldoende bewustwording bij medewerkers door ongeveer de helft van de bedrijven gepercipieerd wordt als het grootste cyberrisico (zie hogerop).

Figuur 5: Adoptiegraad type technische maatregelen (N=2.367)



Beheerprocedures en plannen

De adoptie van een reeks van technische maatregelen is een noodzakelijke maar geen voldoende voorwaarde voor cyberveiligheid. Ondanks alle mogelijke technische maatregelen kan het risico op een cyberincident nooit tot nul herleid worden. Bedrijven die pas nadenken over te ondernemen acties wanneer het cyberincident reeds heeft plaatsgevonden, lopen hopeloos achter de feiten aan te lopen. Aan de hand van beheerprocedures en beleidsplannen denken bedrijven proactief na over hoe cyberincidenten te voorkomen of erop te reageren.

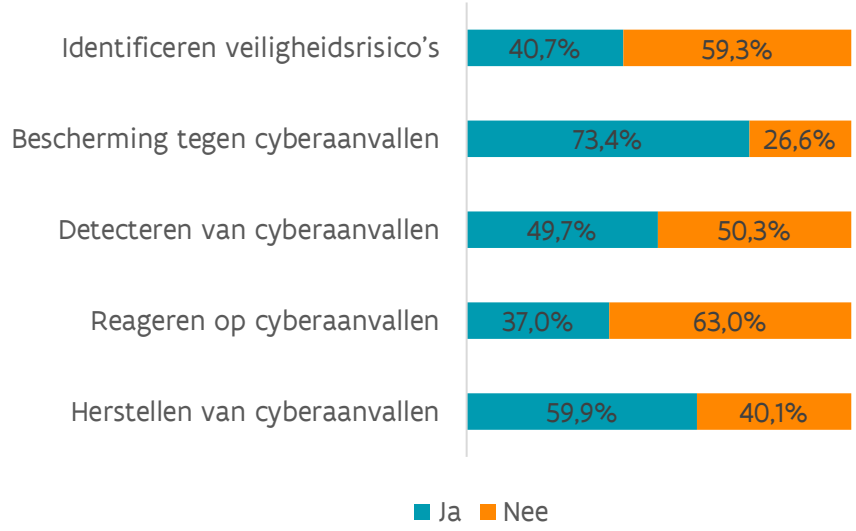
Het NIST-kader biedt een reeks van standaarden, richtlijnen en procedures voor bedrijven om cyberveiligheid te beheren en mogelijke risico's te beperken[9]. NIST bestaat uit vijf elementen van een systematisch cybersecuritybeleid (identificeren, beschermen, detecteren, reageren, herstellen) die cumulatief organisaties helpen cyberaanvallen te identificeren en detecteren, en richtlijnen biedt om preventief en reactief te antwoorden op cyberaanvallen en er van te herstellen. Net zoals bij het nemen van technische maatregelen volstaat het niet om deze of gene beheerprocedure te hebben, maar ligt een adequate cyberbeveiliging in de toepassing van alle vijf elementen: hoe meer procedures een bedrijf instelt, hoe hoger de CS-maturiteit van dat bedrijf.

Ten eerste claimt 40,7% van de bedrijven die ten minste één technische maatregel treffen (i.e. 97,2% van de Vlaamse bedrijven) beheerprocedures te hebben ingevoerd om veiligheidsrisico's binnen het bedrijf te identificeren (zie Figuur 6). Het gaat hierbij bijvoorbeeld om het documenteren van gevoelige databronnen of kritieke bedrijfsprocessen die een mogelijk doelwit zijn bij een eventuele cyberaanval. Ten tweede zegt 73,4% procedures te hebben om zich effectief te beschermen tegen cyberaanvallen, bijvoorbeeld via toegangsbeheer, identificatiemanagement, back-ups, encryptie of regelmatige software-updates. Ten derde heeft 49,7% van de bedrijven die minstens één technische maatregel namen procedures in plaats om cyberaanvallen te detecteren, bijvoorbeeld via continue monitoring van veiligheidsrisico's, technieken en protocollen. Ten vierde zegt 37,0% van deze bedrijven procedures te hebben om adequaat op cyberaanvallen te reageren, bijvoorbeeld aan de hand van incidentanalyses, dreigingseliminatie en/of crisiscommunicatie. Tot slot telt 59,9% van de bedrijven die minstens één technische maatregel namen procedures om te herstellen van een mogelijke cyberaanval (zoals herstel van back-ups, het her-installeren van systemen, het wijzigen van wachtwoorden of firewalls en dergelijke meer).

[9] Voor meer informatie, zie https://www.nist.gov/cyberframework

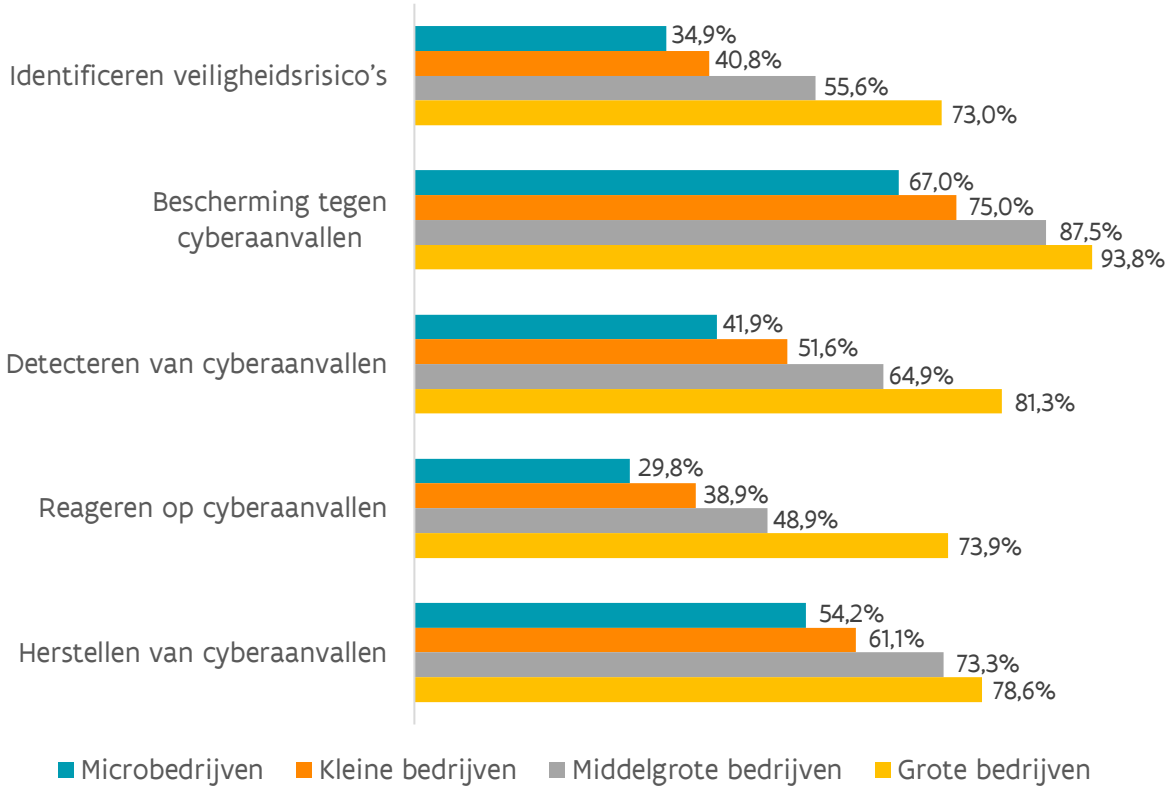
In vergelijking met de meting in 2021 is de implementatie van beheerprocedures ofwel licht gestegen (bescherming tegen en detecteren van cyberaanvallen), ofwel licht gedaald (identificeren van veiligheidsrisico's en reageren op en herstellen van cyberaanvallen) (zie Figuur 24 in Appendix).

Figuur 6: Type beheerprocedures (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



Net zoals bij de technische maatregelen blijkt er een sterk verband tussen het installeren van gerichte beheerprocedures en de bedrijfsgrootte. Ook hier geldt: hoe groter het bedrijf, hoe hoger de kans dat het bedrijf beheerprocedures heeft geïnstalleerd (zie Figuur 7). Zo heeft 73,0% van de grote bedrijven die minstens één technische maatregel namen ook effectief procedures om veiligheidsrisico's te identificeren terwijl dit bij kleine en microbedrijven respectievelijk 40,8% en 34,9% is. 93,8% van de grote bedrijven die minstens één technische maatregel namen heeft procedures om zich te beschermen tegen cyberaanvallen, wat substantieel hoger is dan bij microbedrijven (67,0%). Procedures om cyberaanvallen te detecteren zijn sterker ingeburgerd bij grote bedrijven (81,3%) dan bij kleine (51,6%) en microbedrijven (41,9%). Deze trend is eveneens waarneembaar inzake procedures om te reageren op cyberaanvallen: 73,9% van de grote bedrijven die minstens één technische maatregel namen heeft dergelijke procedures; dit is aanzienlijk hoger dan bij middelgrote bedrijven (48,9%), kleine bedrijven (38,9%) en microbedrijven (29,8%). Tot slot kent 78,6% van de grote bedrijven die minstens één technische maatregel namen procedures om van cyberaanvallen te herstellen terwijl dit bij microbedrijven beperkt blijft tot 54,2%.

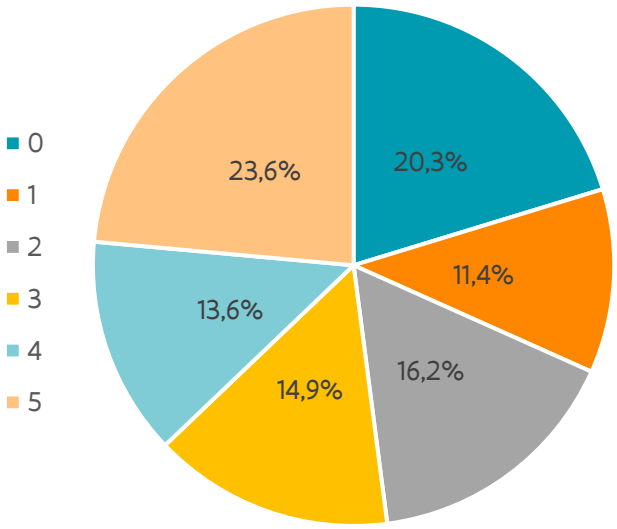
Figuur 7: Type beheerprocedures volgens bedrijfsgrootte (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



Slechts een kwart (23,6%) van de Vlaamse bedrijven die minstens één technische maatregel namen, heeft alle vijf procedures van het NIST-kader in zekere mate geïmplementeerd (zie Figuur 8). Terwijl 54,2% van de grote bedrijven met technische maatregelen en 34,3% van de middelgrote bedrijven met technische maatregelen het NIST-kader toepast, is dit slechts voor 23,0% van de kleine bedrijven en 19,7% van de microbedrijven met technische maatregelen het geval. De sectoren financiële activiteiten en verzekeringen (NACE 64-66) en informatie en communicatie (NACE 58-63) noteren de hoogste scores op dit gebied, met aandelen van respectievelijk 38,9% en 38,0%.

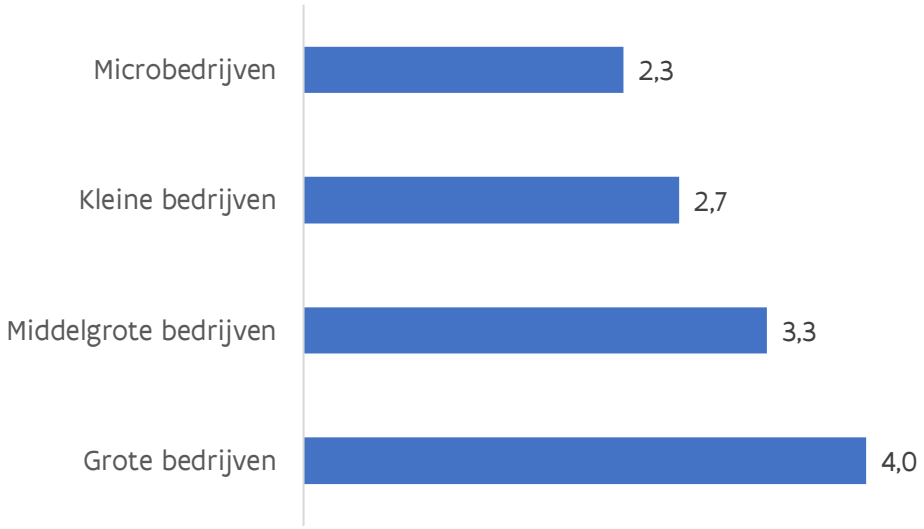
Omgekeerd heeft maar liefst 20,3% van de bedrijven die minstens één technische maatregel namen geen enkele beheerprocedure om zich te beschermen tegen toekomstige cyberrisico's of met actuele cyberaanvallen om te gaan. Dit geldt voor 25,7% van de microbedrijven en 19,0% van de kleine bedrijven die minstens één technische maatregel namen; slechts 8,3% van de middelgrote en 2,7% van de grote bedrijven valt hieronder. Bedrijven actief in accommodatie en maaltijden (NACE 55-56) en de bouwnijverheid (NACE 41-43) vertonen minimale CS-maturiteit; respectievelijk 39,6% en 32,8% van de bedrijven actief in die sector die minstens één technische maatregel namen heeft geen enkele beheerprocedure.

Figuur 8: Aantal beheerprocedures (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



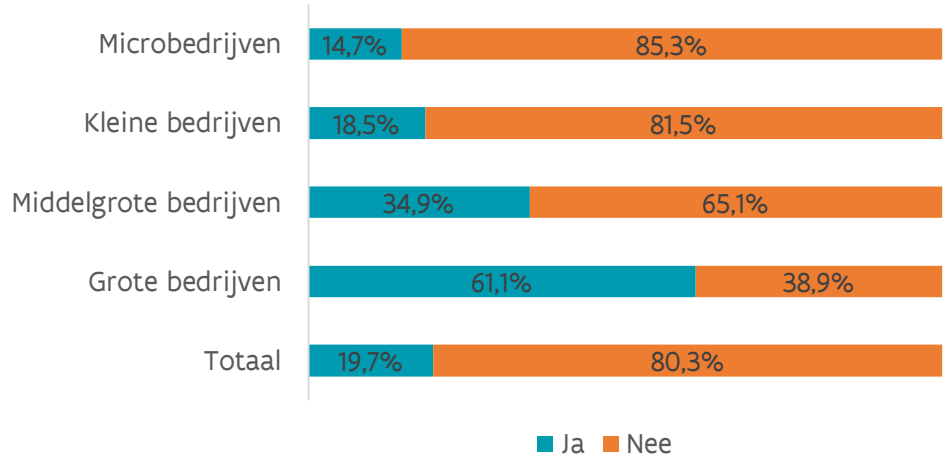
Het belang van bedrijfsgrootte met betrekking tot CS-maturiteit blijkt opnieuw duidelijk uit het gemiddeld aantal beheerprocedures dat bedrijven met technische maatregelen uit verschillende grootteklassen installeren: microbedrijven hebben gemiddeld 2,3 procedures, kleine bedrijven 2,7, middelgrote bedrijven 3,3 en grote bedrijven 4,0 (zie Figuur 9). Grote bedrijven hebben met andere woorden een hogere mate van CS-maturiteit, terwijl kleine en microbedrijven opmerkelijk minder goed beschermd zijn tegen cyberaanvallen.

Figuur 9: Aantal beheerprocedures volgens bedrijfsgrootte (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



De effectiviteit van technische maatregelen en beheerprocedures kan verder verhoogd worden door een doordachte aanpak inzake cybersecurity te formuleren. Het geschikte instrument hiervoor is een beleidsdocument of plan waarin bedrijven een coherent geheel van acties en procedures inzake cybersecurity uitwerken. 19,7% van de bedrijven die ten minste één technische maatregel treffen beschikt over een beleidsdocument inzake cybersecurity (zie Figuur 10). Dit aandeel ligt opmerkelijk hoger bij grote (61,1%) en middelgrote (34,9%) bedrijven. 40,5% van de bedrijven actief in informatie en communicatie (NACE 58-63) en 32,3% van de bedrijven in financiële activiteiten en verzekeringen (NACE 64-66) die minstens één technische maatregel namen heeft effectief een beleidsplan, in tegenstelling tot 11,2% van de bedrijven met technische maatregelen in accommodatie en maaltijden (NACE 55-56) en 6,2% van de bedrijven met technische maatregelen in de bouwnijverheid (NACE 41-43).

Figuur 10: Plan/beleidsdocument inzake cybersecurity volgens bedrijfsgrootte (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



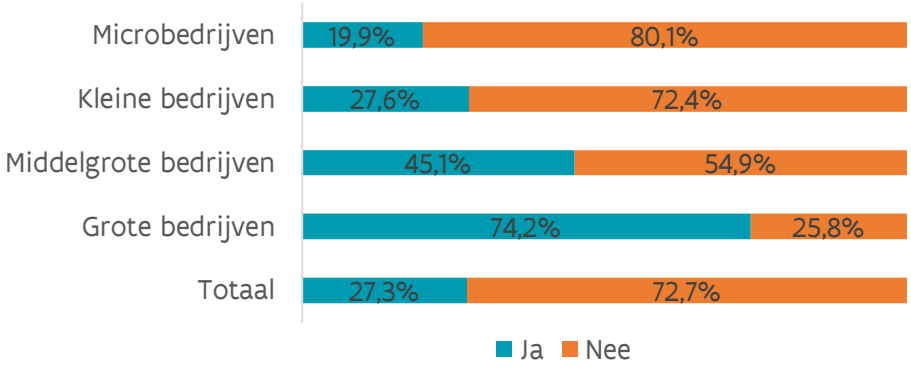
Druk op en vanuit de waardeketen

Als gevolg van de toenemende automatisering en integratie van waardeketens worden elektronische systemen en data almaar vaker gedeeld met leveranciers en klanten. Het directe gevolg hiervan is dat de uiteindelijke mate van bescherming van deze systemen en data bepaald wordt door het bedrijf met de laagste cybermaturiteit. Een ketting is nu eenmaal net zo sterk als de zwakste schakel. Slechts een kwart (27,3%) van de bedrijven in Vlaanderen stelde het afgelopen jaar eisen aan bepaalde of alle leveranciers of onderaannemers inzake cybersecurity (zie Figuur 11).

Dit aandeel ligt een pak hoger bij grote (74,2%) en middelgrote (45,1%) bedrijven dan bij kleinere ondernemingen. Terwijl ongeveer de helft van de bedrijven actief in informatie en communicatie

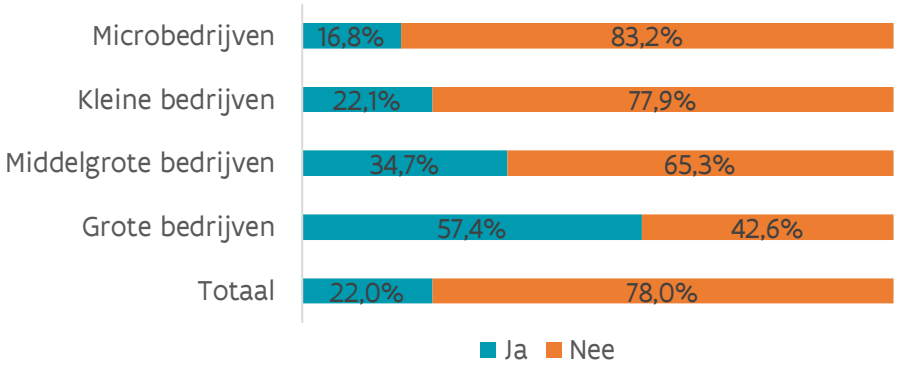
(NACE 58-63) en financiële activiteiten en verzekeringen (NACE 64-66) eisen oplegt aan leveranciers of onderaannemers, is dit slechts het geval voor 13,0% van de bouwbedrijven (NACE 41-43) en 12,5% van de bedrijven actief in accommodatie en maaltijden (NACE 55-56).

Figuur 11: Eisen aan leveranciers/onderaannemers inzake cybersecurity volgens bedrijfsgrootte (N=2.367)



Iets minder dan een kwart (22,0%) van de bedrijven kreeg op zijn beurt eisen opgelegd van bepaalde of alle klanten (zie Figuur 12). Opnieuw ligt dit aandeel beduidend hoger bij grote (57,4%) en middelgrote (34,7%) bedrijven. Maar liefst 74,0% van de bedrijven in informatie en communicatie (NACE 58-63) kreeg eisen opgelegd van klanten.

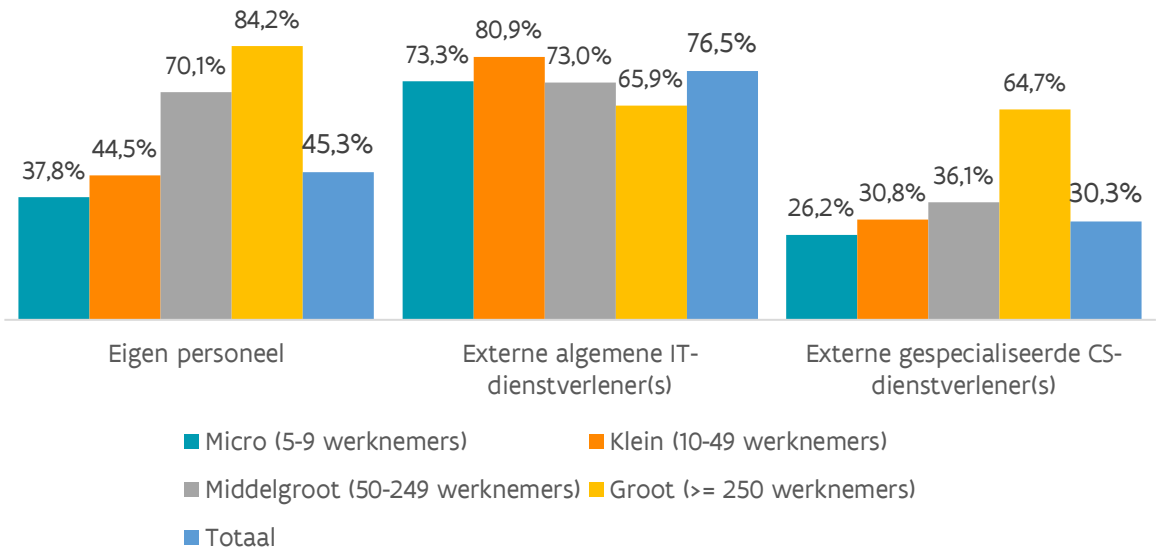
Figuur 12: Eisen van klanten inzake cybersecurity volgens bedrijfsgrootte (N=2.367)



Uitvoering

Zowel het eigen personeel als externe dienstverleners kunnen instaan voor de cybersecurity-activiteiten van bedrijven. Meer dan driekwart (76,5%) van de bedrijven die minstens één technische maatregel namen, doet beroep op externe algemene IT-dienstverleners, 45,3% doet (daarnaast) beroep op het eigen personeel en de minderheid (30,3%) schakelt (daarnaast) externe gespecialiseerde CS-dienstverleners in (zie Figuur 13). Grote bedrijven en middelgrote bedrijven met technische maatregelen maken vaker gebruik van het eigen personeel (respectievelijk 84,2% en 70,1%), terwijl ongeveer twee derde (64,7%) van de grote bedrijven met minstens één technische maatregel aanklopt bij externe gespecialiseerde CS-dienstverleners. Een hoger aandeel (54,9%) bedrijven actief in financiële activiteiten en verzekeringen doet voor hun CS-activiteiten beroep op externe gespecialiseerde CS-dienstverleners, in tegenstelling tot bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening (NACE 86-88) en accommodatie en maaltijden (NACE 55-56) (respectievelijk 19,8% en 18,8%). De overgrote meerderheid (81,7%) van de bedrijven actief in informatie en communicatie (NACE 58-63) schakelt het eigen personeel in, terwijl slechts 33,7% gebruikt maakt van algemene IT-dienstverleners.

Figuur 13: Uitvoering ICT-beveiligingsgerelateerde activiteiten volgens bedrijfsgrootte (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



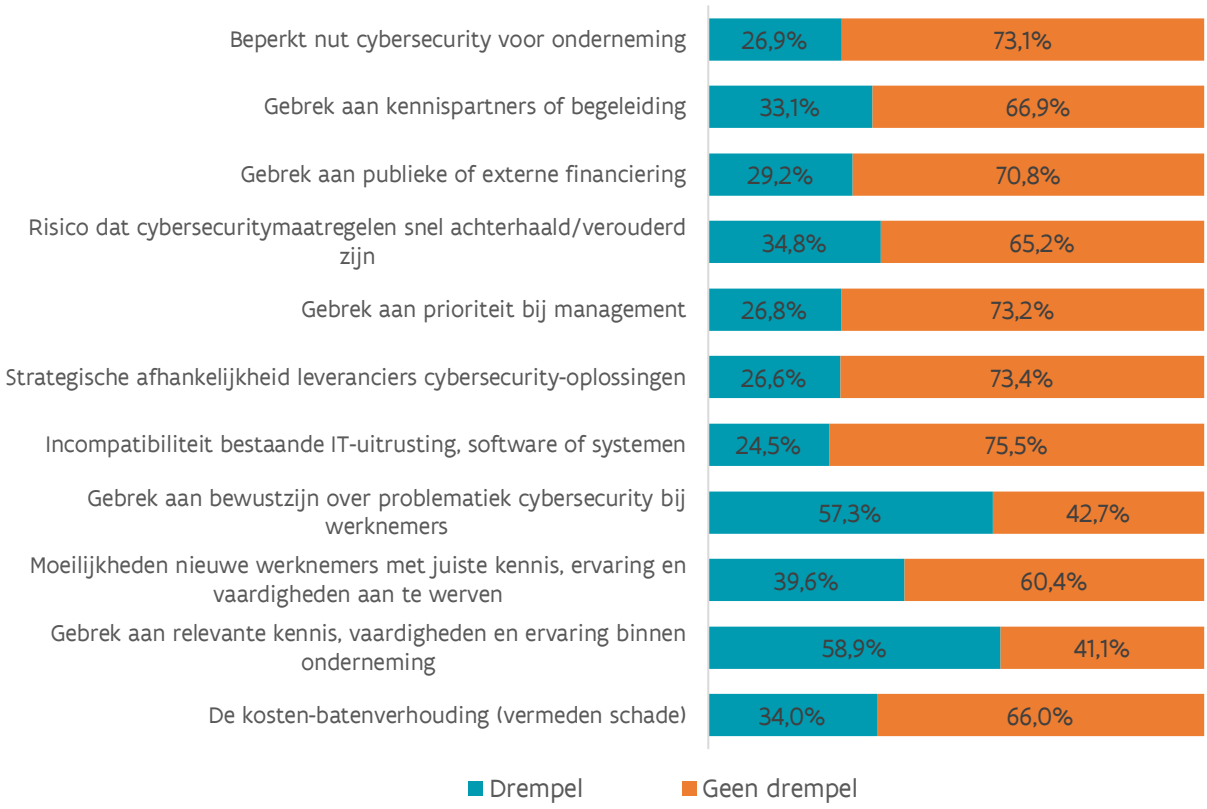
Obstakels

De invoer en het gebruik van technische maatregelen en beheerprocedures stelt bedrijven voor de nodige uitdagingen, die van operationele, financiële, technische of nog andere aard kunnen zijn. Figuur 14 toont welke obstakels bedrijven hierbij ondervinden. 58,9% van de ondernemingen die minstens één technische maatregel invoerden, identificeert het gebrek aan relevante kennis, vaardigheden en ervaring bij de huidige werknemers als een obstakel voor een adequaat CS-beleid; 39,6% ondervindt bovendien moeilijkheden om nieuwe werknemers met deze kennis, vaardigheden en ervaring aan te werven. Behalve kennis en vaardigheden erkent 57,3% van de bedrijven die technische maatregelen namen eveneens een gebrek aan bewustzijn omtrent cybersecurity bij de werknemers. Bedrijven zien het gebrek aan kennis, vaardigheden en bewustzijn met andere woorden als hét belangrijkste obstakel bij de invoer en het gebruik van CS-maatregelen. Nochtans vormt deze menselijke component – naast technische maatregelen en beheerprocedures – een belangrijke verdedigingsgordel tegen cyberaanvallen.

Ongeveer een derde (34,0%) van de bedrijven die minstens één technische maatregel invoerden wijst de kosten-baten (investeringen tegenover de vermeden schade) als obstakel aan; 29,2% wijst een gebrek aan publieke of externe financiering als obstakel aan. 26,8% erkent een gebrek aan prioriteit bij het management als een obstakel voor een effectief CS-beleid. De meerderheid van de bedrijven ziet nochtans de meerwaarde in van het voeren van een CS-beleid voor hun organisatie: ‘slechts’ 26,9% zegt dat ze weinig nut ziet in een dergelijk beleid.

In vergelijking met de meting in 2021 is de mate waarin Vlaamse bedrijven obstakels ondervinden bij de invoer en het gebruik van CS-maatregelen vrijwel uitsluitend toegenomen. De toename is het meest uitgesproken voor het gebrek aan kennis, vaardigheden en bewustzijn (zie Figuur 25 in Appendix).

Figuur 14: Obstakels bij de invoer en het gebruik van CS-maatregelen (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



Omdat slechts 38 bedrijven in de bevraging geen enkele technische maatregel hanteerden, bleek een vergelijking tussen zogenaamde adopters en niet-adopters niet opportuun. Daarom werden bedrijven met een lage adoptiegraad van technische maatregelen (aantal genomen technische maatregelen kleiner dan of gelijk aan 5) (N = 755) en een hoge adoptiegraad van technische maatregelen (aantal genomen technische maatregelen groter dan 5) (N = 1.574) met elkaar vergeleken. Figuur 15 wijst uit dat bedrijven met een lage adoptiegraad meer obstakels ervaren bij de invoer en het gebruik van CS-maatregelen dan bedrijven met een hoge adoptiegraad. Deze ervaren obstakels zijn daarom wellicht ook de redenen voor de lage adoptiegraad.

Bedrijven met een lage adoptiegraad worstelen vaker met een gebrek aan kennis, vaardigheden en ervaring binnen de organisatie (68,1%) dan bedrijven met een hoge adoptiegraad. Bedrijven met een lage adoptiegraad ervaren een sterker gebrek aan kennispartners of begeleiding (47,7%), zien een negatievere kosten-batenverhouding (40,4%) en schatten het nut van een CS-beleid voor hun organisatie lager in (40,4%) dan bedrijven met een hoge adoptiegraad. Eveneens zien we een groter gebrek aan prioriteit bij het management (40,0%) bij bedrijven met een lage adoptiegraad.

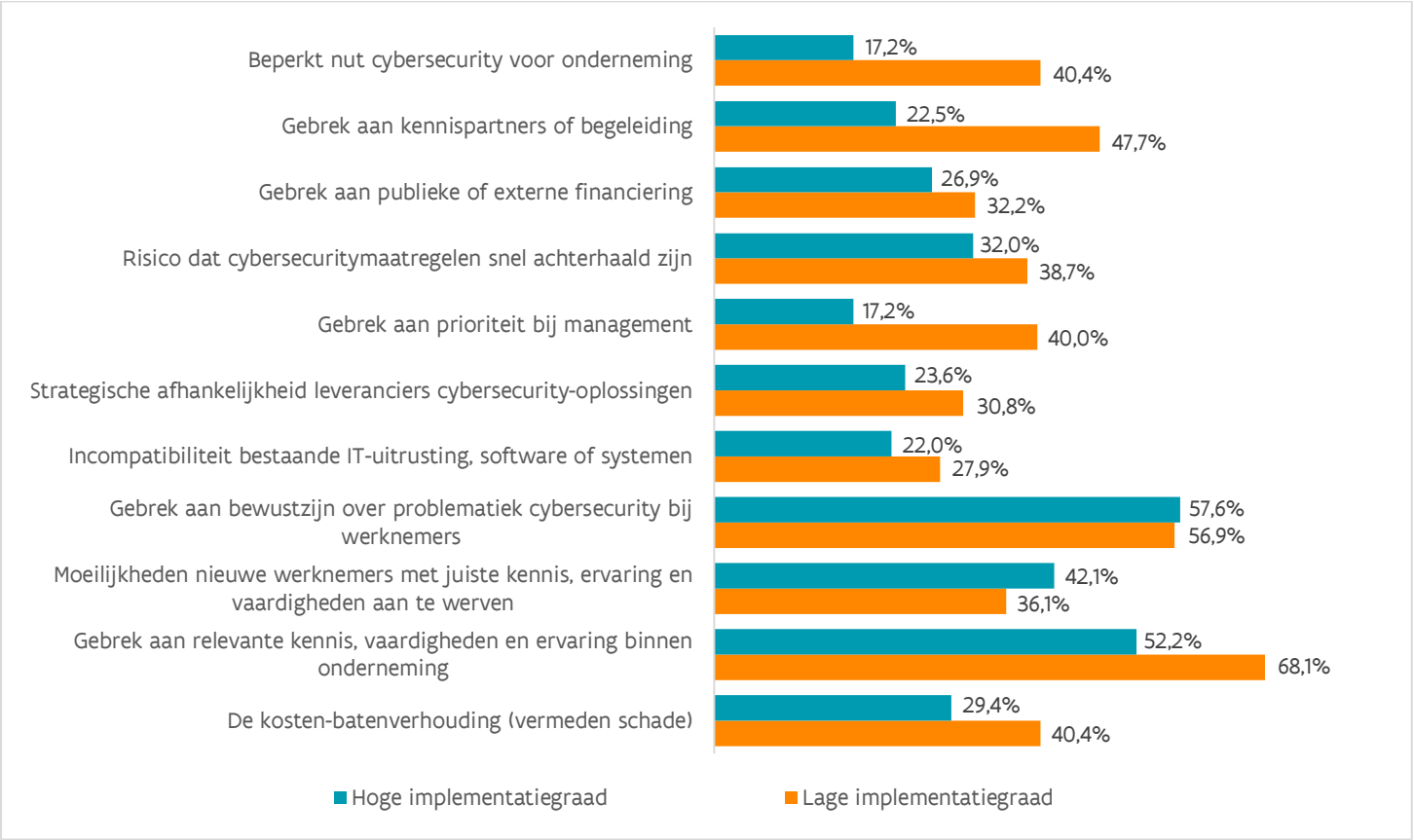
Bedrijven met een hoge adoptiegraad ervaren daarentegen meer moeilijkheden om nieuwe werknemers met de juiste kennis, vaardigheden en ervaring aan te werven. Dit hoeft niet te verwonderen gezien de toepassing van meer en bijgevolg ook meer geavanceerde technische maatregelen meer gespecialiseerde kennis, vaardigheden en kennis vereist.

Beide categorieën van bedrijven ervaren een sterk gebrek aan bewustzijn over de problematiek van cybersecurity bij werknemers. Dit toont aan dat voor Vlaamse bedrijven het menselijke aspect van cybersecurity een belangrijk obstakel vormt bij de invoer en het gebruik van CS-maatregelen, ongeacht de adoptiegraad van technische maatregelen. Het verklaart ook waarom bedrijven zo vaak beroep doen op externe actoren bij de ontwikkeling en implementatie van hun CS-beleid (zie hogerop).

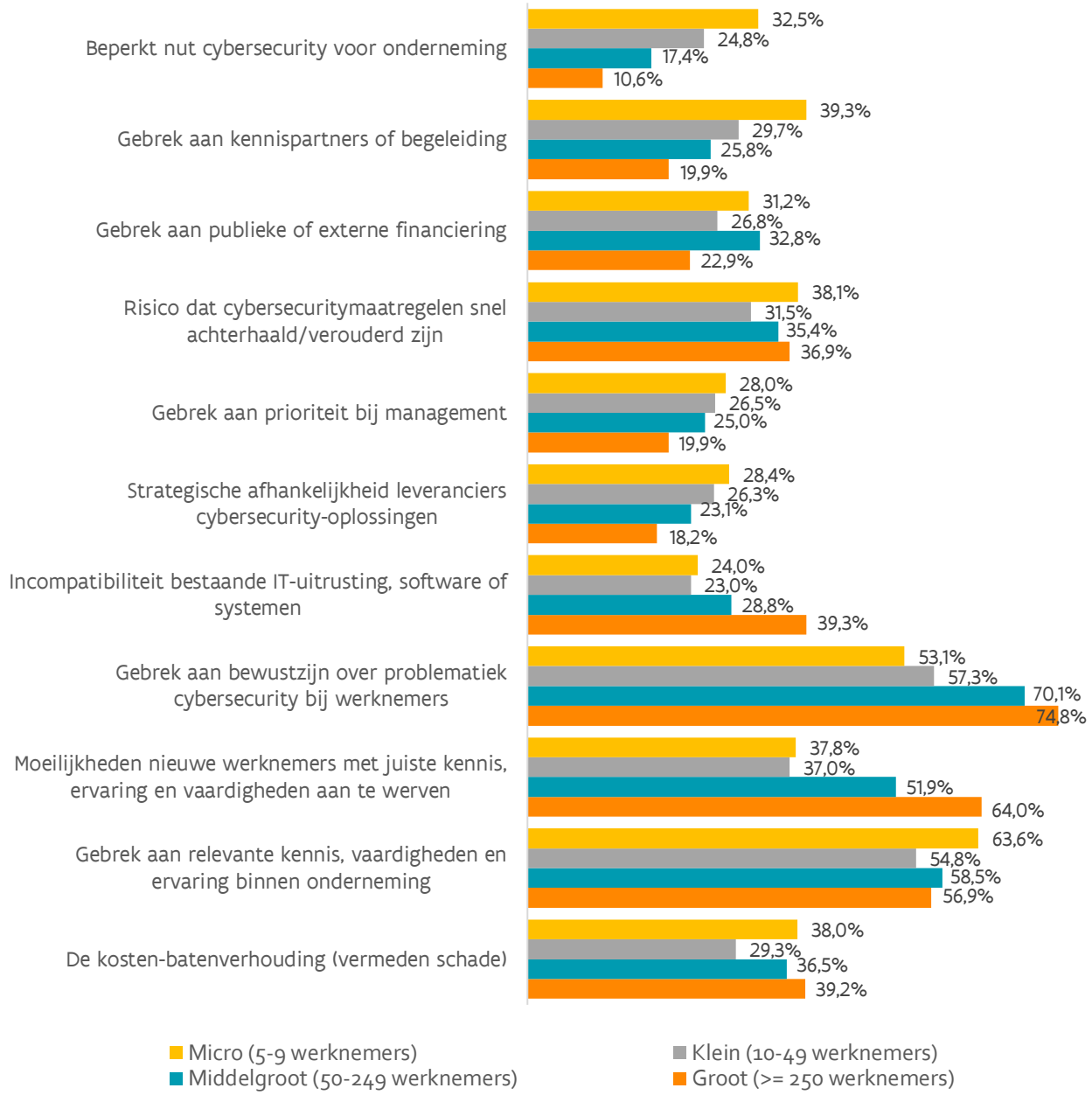
Figuur 16 geeft weer hoe deze obstakels verschillen naargelang de grootteklasse van de onderneming. Voor meer dan de helft van de bedrijven in alle grootteklassen vormt een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming een belangrijk obstakel bij de invoer en het gebruik van CS-maatregelen. Grote en middelgrote bedrijven worstelen daarnaast opmerkelijk vaker dan kleinere bedrijven met een gebrek aan bewustzijn bij werknemers (74,8%) en moeilijkheden om nieuwe werknemers met de juiste kennis, ervaring en vaardigheden aan te werven (64,0%). Microbedrijven en kleine bedrijven ervaren op hun beurt vaker dan grotere bedrijven een gebrek aan kennispartners of begeleiding (39,3%) en schatten het nut van een CS-beleid voor hun organisatie lager in (32,5%).

Voor bedrijven uit om het even welke sector zijn een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming en een gebrek aan bewustzijn bij werknemers twee grote obstakels bij de invoer en het gebruik van CS-maatregelen. Daarbuiten ervaren bedrijven actief in financiële activiteiten en verzekeringen (NACE 64-66) en informatie en communicatie (NACE 58-63) over het algemeen minder vaak obstakels vergeleken met bedrijven uit andere sectoren. Bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening (NACE 86-88) en accommodatie en maaltijden (NACE 55-56) ervaren dan weer vaker obstakels vergeleken met bedrijven uit andere sectoren; bedrijven uit deze twee sectoren wijzen voornamelijk vaker op een gebrek aan publieke of externe financiering, een ongunstige kosten-batenverhouding van een CS-beleid, en een gebrek aan prioriteit bij het management.

Figuur 15: Obstakels bij de invoer en het gebruik van CS-maatregelen volgens adoptiegraad (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



Figuur 16: Obstakels bij de invoer en het gebruik van CS-maatregelen volgens bedrijfsgrootte (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



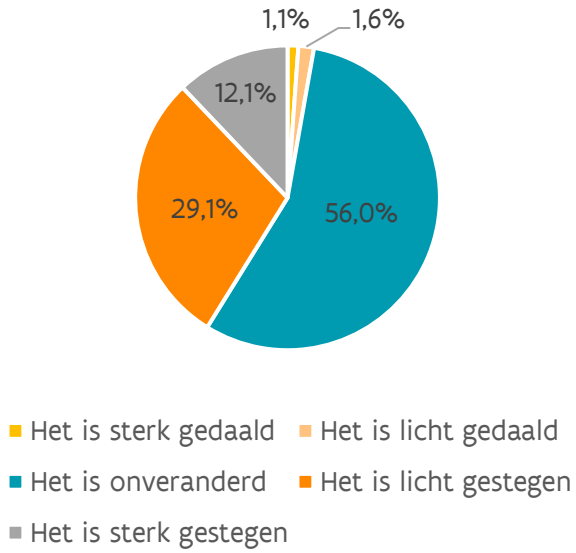
Budget

Bij de meerderheid van de Vlaamse bedrijven die minstens één technische maatregel namen is het budget voor de implementatie van technische maatregelen en beheerprocedures het voorbije jaar onveranderd gebleven dan wel licht gestegen (zie Figuur 17). 41,2% van de bedrijven liet een – lichte of sterke – stijging in de uitgaven voor CS noteren. Voor ongeveer de helft (56,0%) van de bedrijven bleef het budget ongewijzigd. Bij amper 2,8% van de bedrijven daalde het budget het afgelopen jaar. Bijgevolg kunnen we globaal gezien spreken over een stijging in de uitgaven voor CS door Vlaamse bedrijven. De stijging is het sterkst merkbaar bij grote bedrijven; in die groep geeft 49,7% aan dat het budget licht gestegen is terwijl nog eens 29,9% van een sterke toename spreekt. Ook bij middelgrote bedrijven is een stijging meer voorkomend dan bij kleinere ondernemingen: 39,9% voerde een lichte stijging in het CS-budget door, 18,6% spreekt zelfs van een sterke stijging. Bedrijven actief in informatie en communicatie (NACE 58-63), financiële activiteiten en verzekeringen (NACE 64-66), en onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (NACE 68-75) zien hun budgetten het vaakst stijgen; bedrijven actief in accommodatie en maaltijden (NACE 55-56) en de bouwnijverheid (NACE 41-43) het minst.

Gemiddeld spenderen Vlaamse bedrijven naar schatting 19,9% van hun totale IT-budget aan cybersecurity. Bij de grote bedrijven ligt dit gemiddelde lager op 13,8%, bij microbedrijven bedraagt dit gemiddeld 20,3%. Daarbij moet uiteraard gewezen worden op het feit dat eerstgenoemde bedrijven over een groter IT-budget beschikken en het CS-budget dus een groter absoluut bedrag vertegenwoordigt dan de uitgaven van microbedrijven voor CS-maatregelen.

Het aandeel van het CS-budget in het totale IT-budget is licht gedaald ten opzichte van de meting in 2021 (zie Figuur 26 in Appendix). Dit houdt in dat de stijging in het totale IT-budget groter was dan de stijging in de uitgaven voor CS.

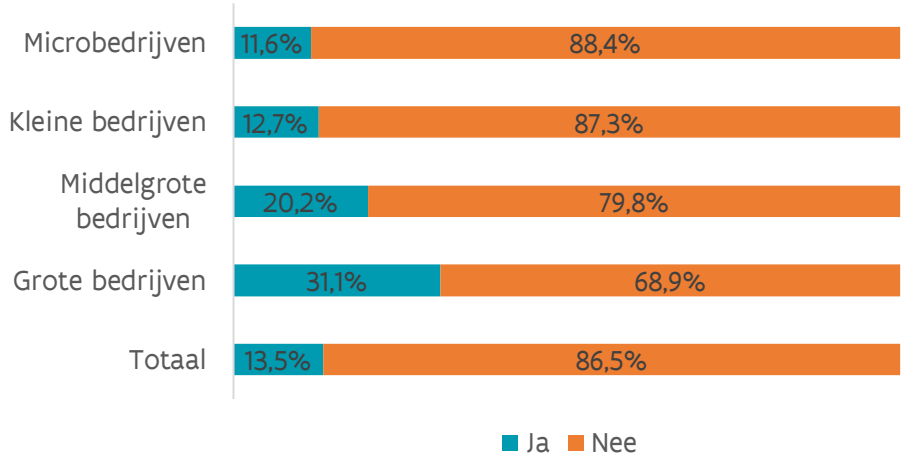
Figuur 17: Evolutie CS-budget (N=2.329) – Deze vraag werd enkel gesteld aan bedrijven die minstens één technische maatregel toepassen



Cyberaanval

De dreiging van cyberrisico's is de afgelopen jaren sterk gestegen. Dit vertaalt zich dan ook in een hoge frequentie van cyberaanvallen op Vlaamse bedrijven: 13,5% van de Vlaamse bedrijven geeft aan het afgelopen jaar het slachtoffer te zijn geweest van een cyberaanval, waarbij cybercriminelen al dan niet met succes trachtten computersystemen onklaar te maken of persoonlijke of confidentiële gegevens te verkrijgen (zie Figuur 18). Dit aandeel is naar alle waarschijnlijkheid een onderschatting van het werkelijke aandeel aangezien (i) een cyberaanval onopgemerkt kan blijven, (ii) respondenten eerder geneigd zijn om zich een cyberaanval te herinneren en deze te rapporteren wanneer de cyberaanval uiteindelijk schade berokkende aan het bedrijf en/of (ii) bedrijven uit vrees voor reputatieschade terughoudend zijn om hierover te communiceren. Grote bedrijven (31,1%) zijn het vaakst slachtoffer van een cyberaanval, ook middelgrote bedrijven (20,2%) worden vaker getroffen. Dit in tegenstelling tot kleine (12,7%) en microbedrijven (11,6%) die in iets mindere mate worden geviseerd door cybercriminelen. Bedrijven actief in administratieve en ondersteunende diensten (NACE 77-82; 95.1) en vervoer en opslag (NACE 49-53) worden opmerkelijk vaker getroffen (respectievelijk 17,8% en 16,6%).

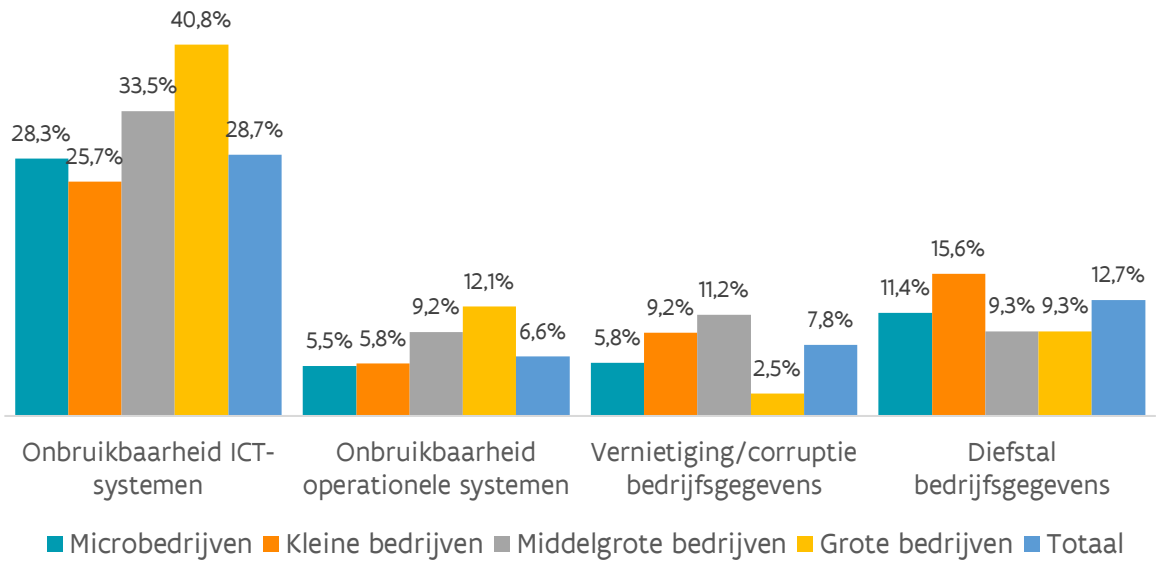
Figuur 18: Slachtoffer van cyberaanval volgens bedrijfsgrootte (N=2.367)



Een dergelijke cyberaanval kan verstrekkende gevolgen hebben voor het getroffen bedrijf. Uit Figuur 19 blijkt dat de *onbruikbaarheid van ICT-systemen* met voorsprong het meest voorkomende operationele gevolg is van een cyberaanval. Bij 28,7% van de geviseerde bedrijven werden ICT-systemen onbruikbaar als gevolg van een cyberaanval, bijvoorbeeld door hacking, kwaadwillige vergrendeling of DDoS-aanval. Dit is in bijzondere mate het geval voor grote bedrijven (40,8%) en middelgrote bedrijven (33,5%), voor bedrijven actief in informatie en communicatie (55,6%), administratieve en ondersteunende diensten (36,5%), en menselijke gezondheidszorg en maatschappelijke dienstverlening (36,0%).

Minder voorkomend is de *onbruikbaarheid van operationele systemen*, zoals machines, gebouwen of andere infrastructuur (6,6%). Ook hier blijken grote bedrijven (12,1%) en middelgrote bedrijven (9,2%) kwetsbaar, net zoals bedrijven actief in informatie en communicatie (19,9%) en menselijke gezondheidszorg en maatschappelijke dienstverlening (12,9%).

Figuur 19: Operationele gevolgen cyberaanval volgens bedrijfsgrootte (N=402) – Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een cyberaanval



7,8% van de bedrijven die een cyberaanval meemaakten werd geconfronteerd met de *vernietiging of het onbruikbaar maken van bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of ongeoorloofde toegang. Hier ervoeren middelgrote en kleine bedrijven de grootste impact van een cyberaanval. In verhouding tot andere sectoren krijgen bedrijven actief in vervoer en opslag (21,6%), informatie en communicatie (13,6%), en accommodatie en maaltijden (13,2%) opmerkelijk vaker met vernietiging van bedrijfsgegevens te maken.

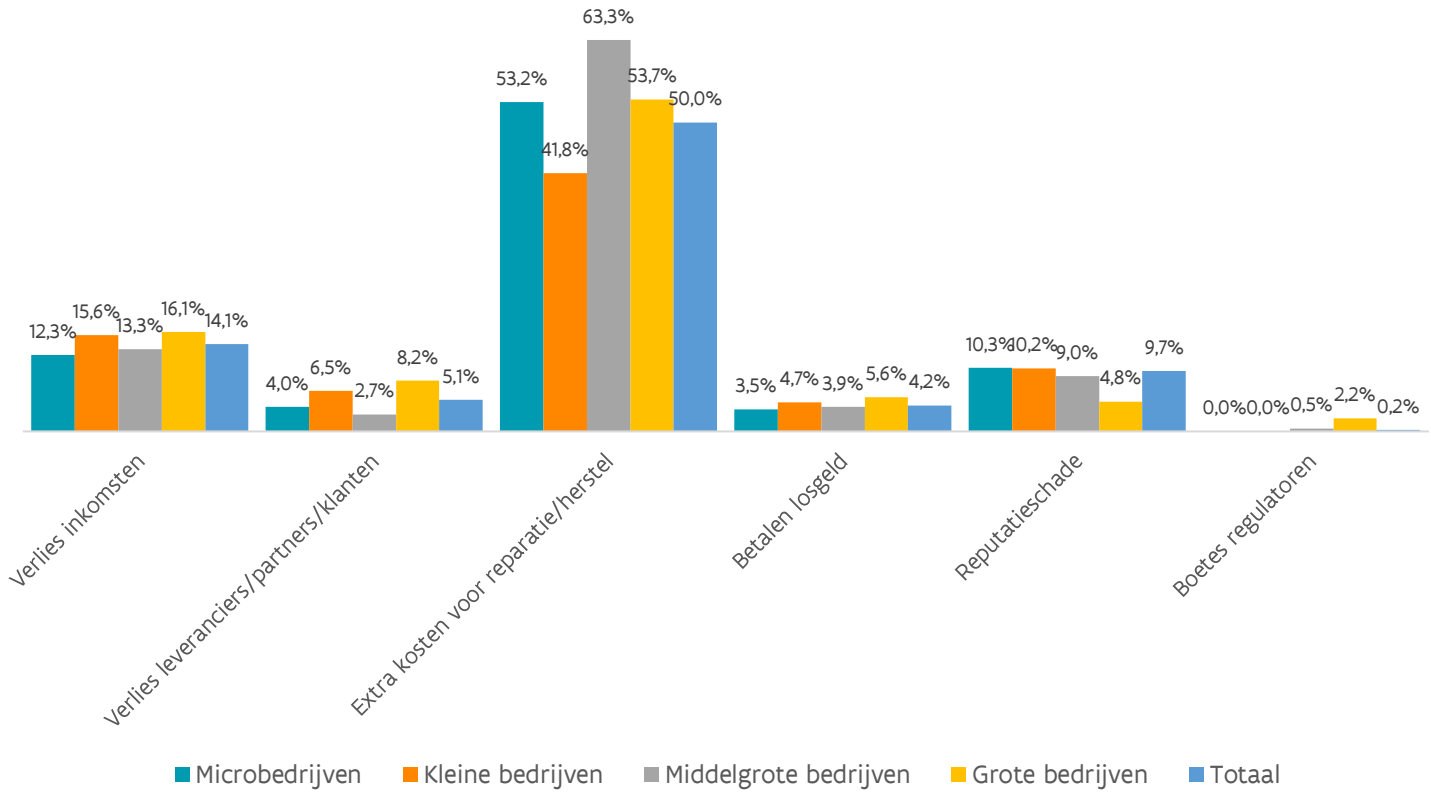
Tot slot kreeg 12,7% van de bedrijven die aangevallen werden te kampen met *diefstal van (confidentiële) bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of phishingberichten. Vooral kleine bedrijven (15,6%) werden hierdoor getroffen, evenals bedrijven actief in vervoer en opslag (20,9%) en accommodatie en maaltijden (15,5%).

Figuur 20 geeft mogelijke andere gevolgen van een cyberaanval weer. De helft (50,0%) van de aangevallen bedrijven geeft aan te lijden onder extra kosten voor reparatie of herstel ten gevolge van de cyberaanval; 14,1% van de bedrijven lijdt inkomstenverlies door een cyberaanval. Reputatieschade (9,7%), verlies van leveranciers, partners of klanten (5,1%), betalen van losgeld (4,2%), en boetes van regulatoren (0,2%) zijn minder voorkomende gevolgen. Bedrijven uit verschillende grootteklassen ondervinden voorgaande gevolgen in min of meer dezelfde mate. Een hoger aandeel bedrijven actief in financiële activiteiten en verzekeringen (74,7%), de nutssector (70,9%), en informatie en communicatie (69,5%) krijgt te maken met extra kosten voor reparatie

of herstel. Verlies van inkomsten is meer voorkomend bij bedrijven actief in vervoer en opslag (32,9%) en informatie en communicatie (25,4%). Reputatieschade voltrekt zich vaker bij bedrijven actief in de bouwnijverheid (23,8%) en vervoer en opslag (21,3%). Verlies van leveranciers, partners of klanten komt vaker voor bij bedrijven actief in financiële activiteiten en verzekeringen (46,9%).

De frequentie van cyberaanvallen op Vlaamse bedrijven is toegenomen ten opzichte van de meting in 2021 (zie Figuur 27 in Appendix). Deze toename vertaalt zich echter niet in een toename van de operationele gevolgen van een cyberaanval: bedrijven werden in vergelijking met de voorgaande meting minder vaak geconfronteerd met de onbruikbaarheid van ICT-systemen, de onbruikbaarheid van operationele systemen, en de vernietiging of het onbruikbaar maken van bedrijfsgegevens (zie Figuur 28 in Appendix). Een logische verklaring hiervoor is dat bedrijven met een lage cybermaturiteit een gemakkelijk slachtoffer vormen voor cybercriminelen. Het aandeel van deze groep bedrijven dat te maken krijgt met operationele gevolgen in geval van een cyberaanval is hoog. Naarmate ook bedrijven met een hogere cybermaturiteit geviseerd worden door cybercriminelen, stijgt weliswaar het aandeel slachtoffers maar daalt het aandeel bedrijven dat te maken krijgt met operationele gevolgen als gevolg van de hogere gemiddelde cybermaturiteit. Niettegenstaande is het aandeel aangevallen bedrijven dat te maken kreeg met diefstal van (confidentiële) bedrijfsgegevens gestabiliseerd.

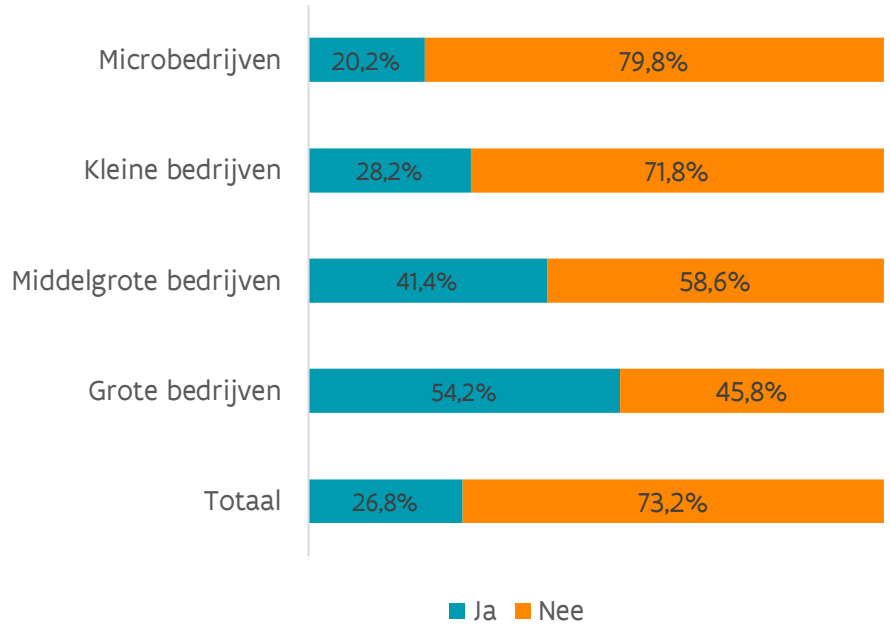
Figuur 20: Andere gevolgen cyberaanval volgens bedrijfsgrootte (N=402) – Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een cyberaanval



Meer dan een kwart van de Vlaamse bedrijven (26,8%) is verzekerd tegen cyberaanvallen (zie Figuur 21). Een dergelijke verzekering dekt (gedeeltelijk) de financiële schade van een geslaagde cyberaanval (zoals bijvoorbeeld losgeld of schade bij derden) maar verlaagt het risico op een cyberaanval uiteraard niet. Bedrijven blijven ondanks een verzekering tegen cyberaanvallen even kwetsbaar bij gebrek aan technische maatregelen en beheerprocedures. Van de grote bedrijven claimt meer dan de helft (54,2%) een verzekering afgesloten te hebben tegen cyberaanvallen. Dit aandeel ligt een pak lager bij de middelgrote bedrijven (41,4%), de kleine bedrijven (28,2%), en de microbedrijven (20,2%). Terwijl een opmerkelijk hoger aandeel bedrijven actief in informatie en communicatie en financiële activiteiten en verzekeringen verzekerd is (respectievelijk 46,4% en 45,4%), geldt het omgekeerde voor accommodatie en maaltijden (11,5%).

In vergelijking met de meting in 2021 is het aandeel tegen cyberaanvallen verzekerde bedrijven licht gestegen (zie Figuur 29 in Appendix).

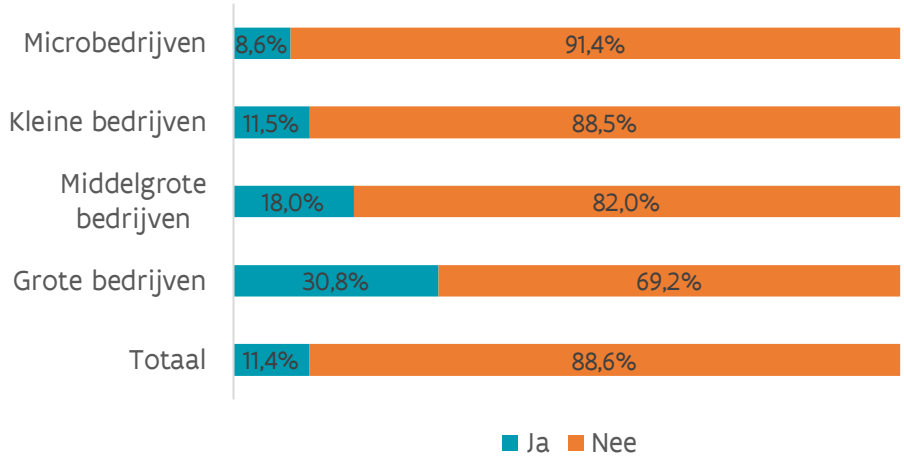
Figuur 21: Verzekering tegen cyberaanvallen volgens bedrijfsgrootte (N=2.367)



Overheidsbeleid

In maart 2019 lanceerde de Vlaamse overheid het *Vlaams Actieplan Cybersecurity* met de ambitie om cyberveiligheid in Vlaamse bedrijven een topprioriteit te maken. Het plan bestaat uit drie luiken: (1) onderzoek, (2) gebruik van CS-oplossingen door bedrijven en (3) bewustmaking en opleiding. Het speelt hiermee duidelijk in om een aantal van de hierboven gedocumenteerde struikelblokken. Gevraagd naar het bestaan van dit actieplan zegt 11,4% van de Vlaamse bedrijven weet te hebben van dit beleidsplan; 88,6% daarentegen stelt niet op de hoogte te zijn (zie Figuur 22). Het aandeel bedrijven dat kennis heeft van het actieplan is hoger voor grote bedrijven (30,8%) en middelgrote bedrijven (18,0%) dan voor kleine bedrijven (11,5%) en microbedrijven (8,6%). Vooral bedrijven actief in informatie en communicatie (20,4%) en financiële activiteiten en verzekeringen (16,0%) zijn op de hoogte van het actieplan, in tegenstelling tot bedrijven actief in accommodatie en maaltijden (8,2%) en menselijke gezondheidszorg en maatschappelijke dienstverlening (7,8%).

Figuur 22: Kennis specifiek actieplan Vlaamse overheid volgens bedrijfsgrootte (N=2.367)



Conclusies

Deze studie heeft als doel om de CS-maturiteit van Vlaamse bedrijven in kaart te brengen. De CS-maturiteit van een bedrijf wordt bepaald door de combinatie van technische maatregelen, beheerprocedures, en de kennis en het bewustzijn omtrent cybersecurity bij het management en werknemers (en bij uitbreiding, leveranciers). De meerderheid van de Vlaamse bedrijven neemt verschillende technische maatregelen, hoewel deze vaak beperkt blijven tot relatieve basismaatregelen zoals software-updates en data back-ups. Slecht een minderheid neemt meer geavanceerde technische maatregelen zoals het bijhouden van log files om cyberaanvallen te analyseren, periode ICT-veiligheidsanalyse, ICT-veiligheidstesten of encryptietechnieken voor data, documenten of e-mails. De adoptie van beheerprocedures in Vlaamse bedrijven is ook weinig verspreid. Slechts een kwart van de bedrijven die technische maatregelen namen heeft de vijf procedures van het NIST-kader (identificeren, beschermen, detecteren, reageren, herstellen) in zekere mate geïmplementeerd; één op vijf heeft zelfs geen enkele beheerprocedure.

Hoewel bijna driekwart van de Vlaamse bedrijven meent goed beschermd te zijn tegen cyberaanvallen, liggen de zaken volgens bovenstaande bevindingen eerder anders. De afwezigheid van geavanceerde technische maatregelen en beheerprocedures wijzen in de richting van het uitblijven van een algemene hoge CS-maturiteit. Als belangrijkste obstakels bij de invoer en het gebruik van CS-maatregelen haalt de meerderheid van de bedrijven zowel een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming als een gebrek aan bewustzijn over de problematiek rond cybersecurity bij werknemers aan. Ook de prioritering door het management blijft een werkpunt. Mogelijke oplossingen voor deze obstakels, zoals het organiseren van opleidingen of activiteiten voor medewerkers, worden echter zelden door bedrijven aangegrepen. Dit leidt tot een situatie waarin bijna de helft van de bedrijven onvoldoende bewustwording bij medewerkers als zijn grootste cyberrisico beschouwt.

Een lage CS-maturiteit als gevolg van (de combinatie) van onvoldoende technische maatregelen, beheerprocedures, of kennis en bewustzijn maakt bedrijven meer kwetsbaar voor cyberaanvallen. 13,5% van de Vlaamse bedrijven gaf aan het afgelopen jaar slachtoffer te zijn van een cyberaanval. Dit percentage is zeer waarschijnlijk nog een onderschatting. Hoewel de gevolgen van cyberaanvallen in de meeste gevallen beperkt blijven tot de onbruikbaarheid en het herstel van ICT-systemen, moeten bedrijven rekening houden met mogelijk verstrekkende gevolgen.

Ondanks de vaststelling dat de uitgaven voor CS door Vlaamse bedrijven het afgelopen jaar zijn gestegen, wijst deze studie vooral op de nood aan bijkomende investeringen met het oog op het bereiken van een hoge CS-maturiteit. De adoptie van meer en vooral meer geavanceerde technische maatregelen, het uitwerken van beheerprocedures, en een inzet op bewustmaking bij medewerkers én management zijn hierbij een absolute must. Het opstellen van een coherent plan of beleidsdocument is in deze een extra troef.

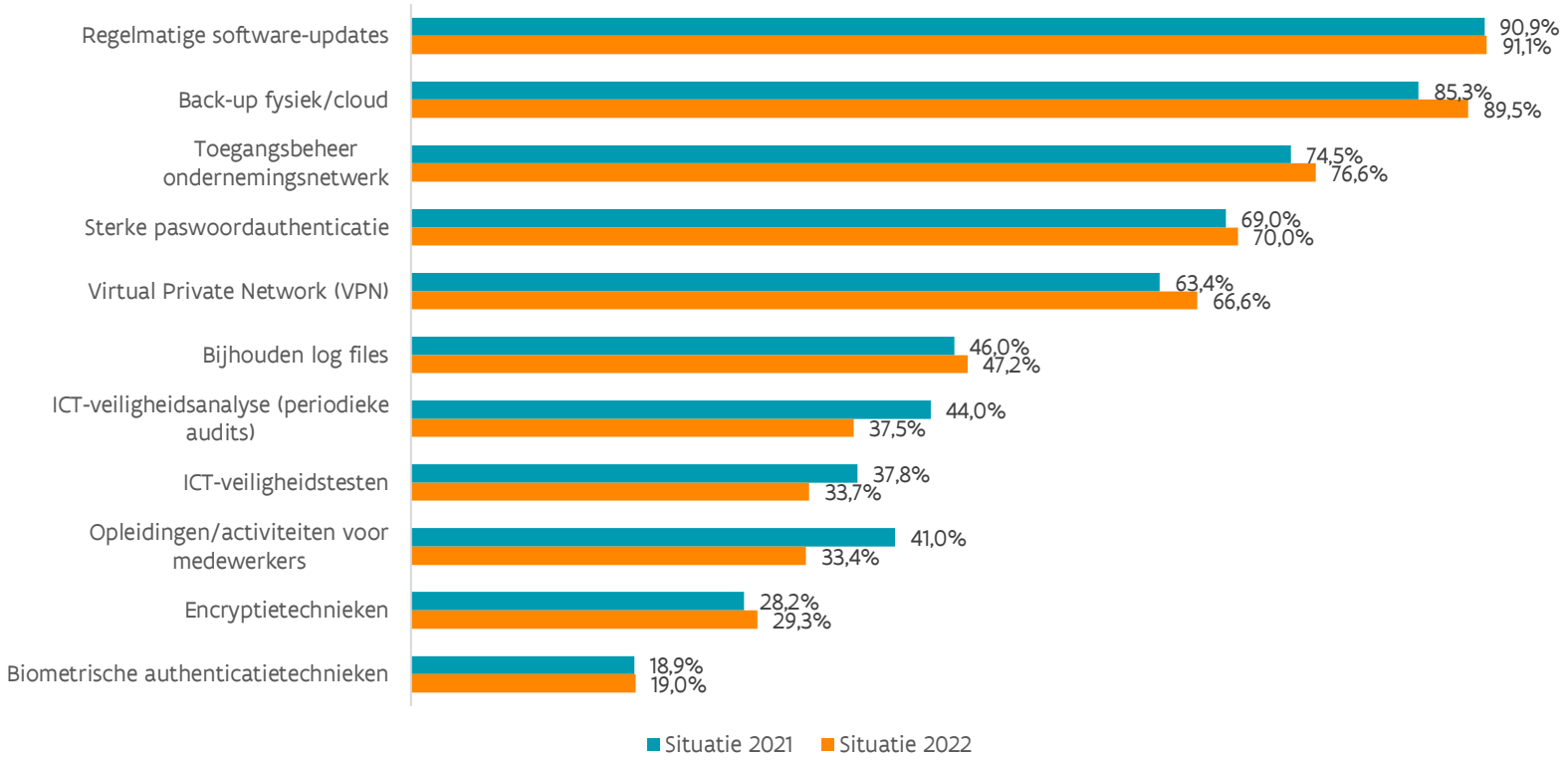
Deze bevindingen, in combinatie met de vrij beperkte bekendheid van bedrijven met het *Vlaams Beleidsplan Cybersecurity*, wijzen op de blijvende nood aan initiatieven die als doel hebben te informeren en sensibiliseren. Daarnaast ervaart ongeveer de helft van Vlaamse bedrijven met een lage adoptiegraad van technische CS-maatregelen een gebrek aan kennispartners of begeleiding als obstakel bij de invoer en het gebruik van (bijkomende) maatregelen ter zake. Het overheidsbeleid moet bijgevolg ook blijven inzetten op het stimuleren van samenwerkingsverbanden tussen ondernemingen. Samenwerking en uitbesteding van cybersecurity-activiteiten kunnen immers ten dele compenseren voor het gebrek aan interne gespecialiseerde kennis rond cyberveiligheid. Het merendeel van de Vlaamse bedrijven die CS-maatregelen namen, schakelt hiervoor externe algemene IT-dienstverleners in. Externe gespecialiseerde CS-dienstverleners worden echter in veel mindere mate geconsulteerd, hoewel zij net een grote meerwaarde kunnen leveren bij de invoer en het gebruik van CS-maatregelen in bedrijven.

Appendix

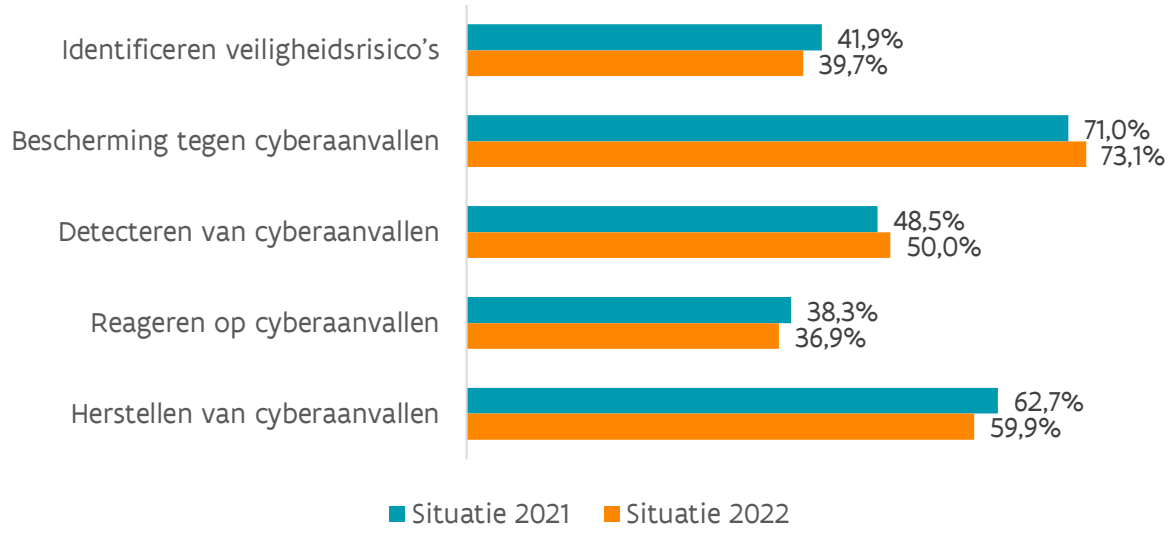
Tabel 3: Geselecteerde sectoren

NACE-codes	Omschrijving
NACE 10-33	Maakindustrie
NACE 35-39	Productie en distributie van elektriciteit, gas, stoom en gekoelde lucht; distributie van water; afval- en afvalwaterbeheer en sanering
NACE 41-43	Bouwnijverheid
NACE 45-47	Groothandel en detailhandel; reparatie van auto's en motorfietsen
NACE 49-53	Vervoer en opslag
NACE 55-56	Accommodatie en maaltijden
NACE 58-63	Informatie en communicatie
NACE 64-66	Financiële activiteiten en verzekeringen
NACE 68-75	Exploitatie van en handel in onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten
NACE 77-82	Administratieve en ondersteunende diensten
NACE 86-88	Menselijke gezondheidszorg en maatschappelijke dienstverlening
NACE 95.1	Reparatie van computers en communicatieapparatuur

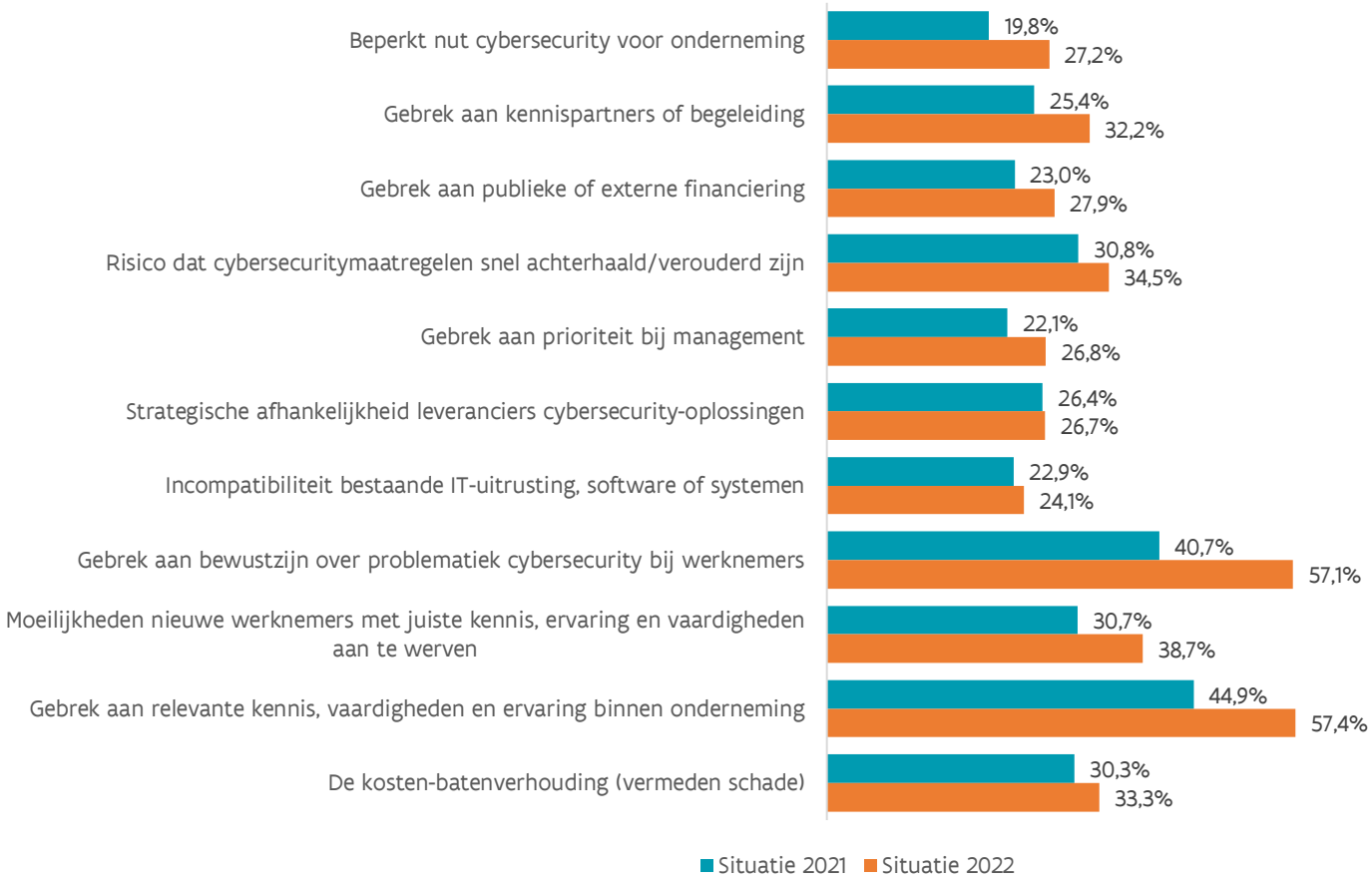
Figuur 23: Evolutie adoptiegraad technische maatregelen volgens type



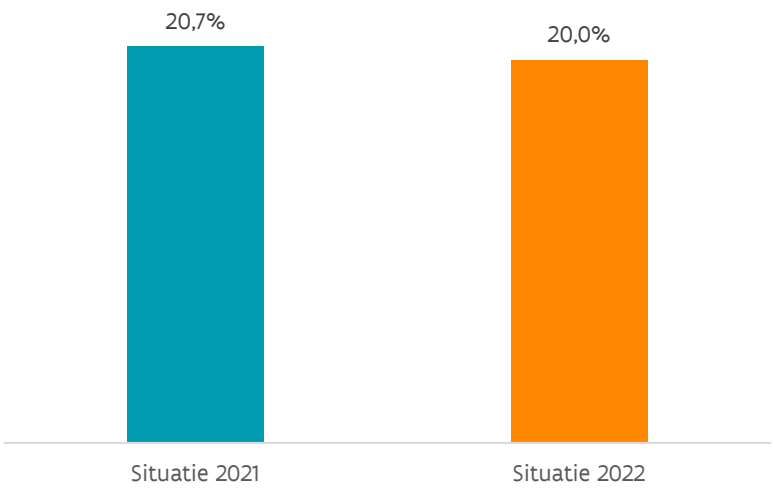
Figuur 24: Evolutie implementatie beheerprocedures volgens type



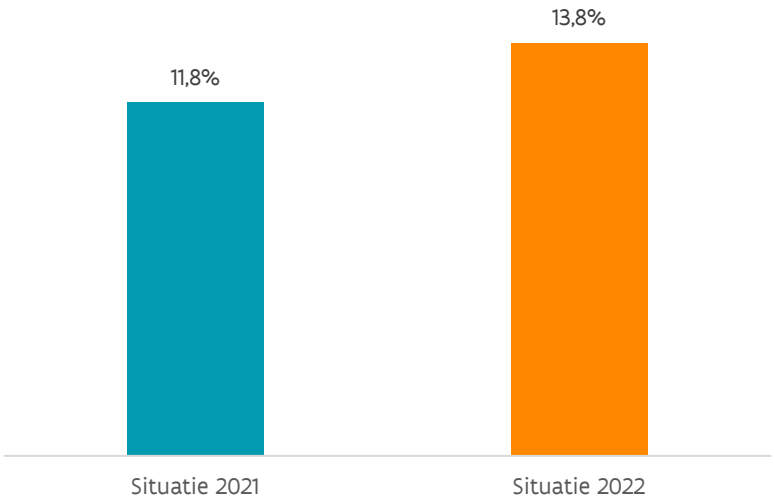
Figuur 25: Evolutie aandeel bedrijven dat obstakels ondervond bij de invoer en het gebruik van CS-maatregelen



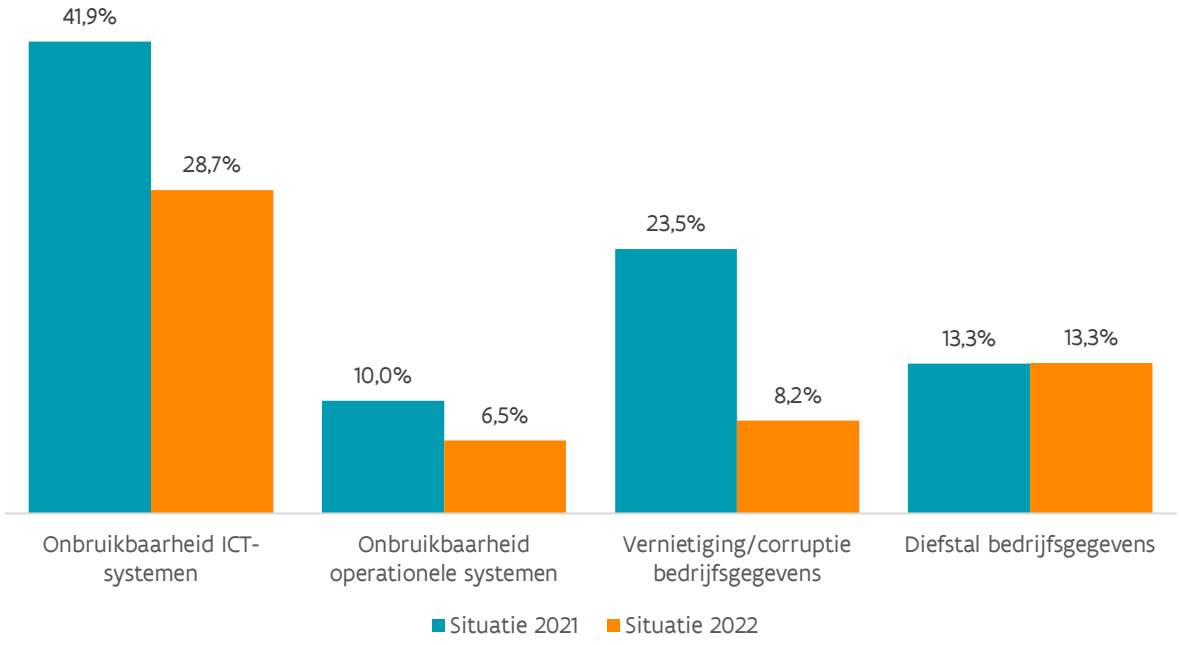
Figuur 26: Evolutie aandeel van het IT-budget gespendeerd aan cybersecurity



Figuur 27: Evolutie aandeel bedrijven dat het slachtoffer was van een cyberaanval



Figuur 28: Evolutie frequentie operationele gevolgen bij slachtoffers van een cyberaanval



Figuur 29: Evolutie aandeel bedrijven met een verzekering tegen cyberaanvallen