motivaction
insights and strategy

Cybersecurity verwachtingen onder IT-afnemers en IT-dienstverleners

M241040

Kevin Hengstz
Daniëlle van Velzen

22-4-2025

k.hengstz@motivaction.nl
d.vanvelzen@motivaction.nl

Inhoud

motivaction
insights and strategy

Achtergrond

In opdracht het Digital Trust Center (hierna: DTC) van het ministerie van Economische Zaken, heeft Motivaction International bv een onderzoek uitgevoerd naar de verwachtingen ten aanzien van cybersecurity onder IT-afnemers en IT-dienstverleners.

Cybersecurity verwachtingen
In toenemende mate werken bedrijven in complexe ecosystemen met meerdere IT-leveranciers. Maar wie zorgt ervoor dat alles *secure* blijft? Is dat het bedrijf, de IT-afnemer zelf? Of liggen er ook verantwoordelijkheden bij de IT-leveranciers? In sommige gevallen worden er duidelijke afspraken gemaakt en worden de verwachtingen over-en-weer uitgesproken. Dit is echter niet altijd het geval; soms is niet alles vastgelegd en zijn er toch verwachtingen.

Duidelijkheid & verantwoordelijkheid
Met dit onderzoek wil het Digital Trust Center inzicht krijgen in de veronderstelde onduidelijkheden op het gebied van cybersecurity in de relatie tussen IT-afnemers en IT-leveranciers. Door inzicht te geven in de cybersecurity-verwachtingen van beide partijen, verwacht het Digital Trust Center deze twee partijen dichter bij elkaar te brengen brengen. Het is belangrijk dat deze twee partijen met elkaar duidelijkheid creëren over wie precies waarvoor verantwoordelijk is. Als er duidelijk is, is de kans groter dat de partijen goed op elkaar zijn afgestemd in het geval van een cyberaanval. Dan is de kans groter dat ze de cyberaanval kunnen afslaan.

Methode en opzet

Methode, doelgroep en steekproef
Het onderzoek is uitgevoerd door middel van een online vragenlijst onder een steekproef van netto n=278 IT-dienstverleners en n=420 IT-afnemers uit het Nederlandse bedrijfsleven. De respondenten zijn merendeels afkomstig uit het StemPunt-panel van Motivaction en een panel van een partner.

IT-dienstverleners voldoen aan de selectiecriteria als zij:
1) ICT-diensten leveren aan zakelijke klanten, en
2) Invloed hebben in hun bedrijf op één of meer van de volgende onderdelen: het managen van de relatie met klanten; het opvangen/oplossen van cyber-calamiteiten bij klanten; het opstellen van de contracten/SLA's waarin de verantwoordelijkheid voor digitale veiligheid met klanten is geregeld, en
3) Minimaal één van de volgende diensten leveren: Cloud & Datacenter Services, Werkplek & End-user Services, Software Services, Security Services, Platform & Data Services

IT-afnemers voldoen aan de selectiecriteria als zij:
1) ICT-diensten afnemen bij IT-dienstverleners, en
2) Invloed hebben in hun bedrijf op het managen van de IT beveiliging en de cyberveiligheid van de organisatie, en
3) Minimaal één van de volgende diensten afnemen: Cloud & Datacenter Services, Werkplek & End-user Services, Software Services, Security Services, Platform & Data Services

Veldwerk
Het veldwerk is uitgevoerd van 20 februari t/m 10 maart 2025.

Leeswijzer
De resultaten worden steeds op totaalniveau (alle dienstverleners en afnemers) weergegeven. De verschillen tussen dienstverleners en afnemers worden tekstueel benoemd en worden getoond in de grafieken. In de grafiek geven we significante verschillen aan met een pijl omhoog ⇧ (vaker genoemd door IT-dienstverleners dan door IT-afnemers) of een pijl omlaag ⇩ (minder vaak genoemd door IT-dienstverleners dan door IT-afnemers).

Daarnaast benoemen we tekstueel ook significante verschillen op basis van het Cyberveilig profiel van de organisatie van de afnemers (zie omschrijvingen op p.5). Daarbij onderscheiden we de volgende groepen:
- Digitaal veilige afnemers, n=97
- Digitaal waakzame afnemers, n=123
- Digitaal overmoedige afnemers, n=51
- Praktisch digitale afnemers, n=149

Omwille van de leesbaarheid van de grafieken worden percentages lager dan 3% niet vermeld in de grafiek.

De vraagstelling voor dienstverleners verschilde op sommige punten van de vraagstelling voor afnemers. In het rapport zijn zowel de vraagstelling voor dienstverleners als de vraagstelling voor afnemers opgenomen.

Self assessment: Cyberveilig profiel organisatie

Dienstverleners: **Als je de bedrijven waar jullie IT-diensten aan leveren zou moeten typeren op het gebied van digitale veiligheid (cybersecurity) en IT-beveiliging; welke van de onderstaande beschrijvingen past over het algemeen dan het beste?**

Afnemers: **Als je het bedrijf waar je werkt zou moeten typeren op het gebied van digitale veiligheid (cybersecurity) en IT-beveiliging; welke van de onderstaande beschrijvingen past dan het beste?**

Digitaal veilig (bewust – bekwaam)

We zijn ons bewust van de digitale gevaren die ons bedrijf loopt.
Wij zijn volledig up-to-date op het gebied van digitale veiligheid (cybersecurity).
We hebben ons goed voorbereid (mensen trainen én processen inrichten) op een mogelijke cyberaanval.

Digitaal waakzaam (bewust – onbekwaam)

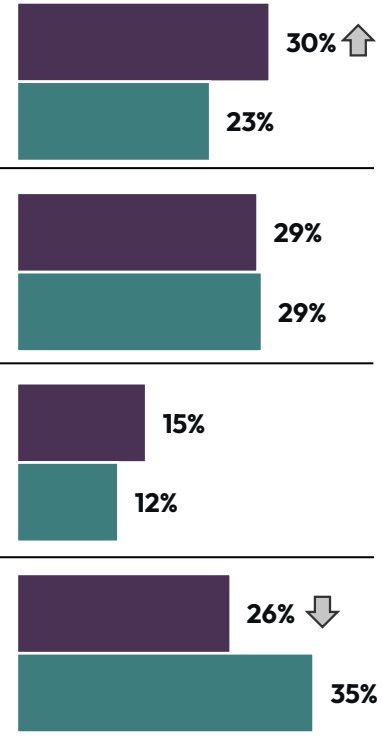
We zijn ons bewust dat ons bedrijf digitaal gevaar kan lopen.
We doen ons best op het gebied van digitale veiligheid (cybersecurity), maar weten dat het beter kan en misschien wel zou moeten.
Er zijn overwegingen waarom we er niet alles aan doen, daarom voelen we ons niet 100% veilig en zijn we waakzaam.

Digitaal overmoedig (onbewust – bekwaam)

We zijn een 'tech savvy' bedrijf;
Alle mensen die bij ons werken zijn heel goed op de hoogte van alle digitale gevaren.
Mocht het dan toch een keer misgaan, dan is er voldoende IT-kennis in huis om het probleem op te lossen en/of de juiste mensen in te schakelen.

Praktisch digitaal (onbewust – onbekwaam)

Het is net als in het echte leven; je moet gewoon je gezonde verstand gebruiken. Niet op links klikken van onbetrouwbare afzenders etc.
En verder goed je updates bijhouden en een virusscanner gebruiken.
Mocht het dan toch mis gaan, dan zien we dan wel. Je kunt je toch niet overal op voorbereiden.



⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

CONCLUSIE

motivaction
insights and strategy

Qua cyberkennis leunen IT-afnemers op de expertise van de IT-dienstverleners. IT-dienstverleners kijken vaker hiervoor naar de overheid. Zowel IT-dienstverleners als IT-afnemers maken zich zorgen om hun digitale veiligheid, ze zijn nog niet volledig voorbereid op cyberincidenten. Met name de afstemming tussen betrokken partijen is nog niet optimaal: er is geen consensus over de mate van afstemming tussen IT-dienstverleners en IT-afnemers. Deze afstemming is juist van groot belang. IT-dienstverleners en IT-afnemers vinden namelijk dat ze gedeelde verantwoordelijkheid hebben voor de digitale veiligheid van IT-afnemers. Hierdoor ligt onduidelijkheid op de loer; gedeelde verantwoordelijkheid kan leiden tot geen verantwoordelijkheid.

Cyberveilige houdingen: Cyberzorgen

Grote zorgen over cyberveiligheid afnemers

- Veel IT-dienstverleners (79%) maken zich (zeer veel) zorgen om de digitale veiligheid van hun afnemers. Veel, maar minder, afnemers (60%) maken zich (zeer veel) zorgen om de digitale veiligheid van hun bedrijf.

Zelfvertrouwen en vertrouwen in elkaar voornaamste redenen voor partijen om zich geen of weinig zorgen te maken om digitale veiligheid

- IT-dienstverleners geven aan zich geen of weinig zorgen te maken, omdat ze vertrouwen hebben in de maatregelen die zij als dienstverlener hebben genomen (64%).
- Afnemers hebben enerzijds vertrouwen in hun IT-dienstverlener (43%) en anderzijds denken ze genoeg maatregelen te hebben getroffen om een cyberincident te voorkomen (46%).

Cyberveilig gedrag: Cyberreadiness afstemming

Vertrouwen is goed, voorbereiden is beter

- De partijen die zich slecht of niet gezamenlijk voorbereiden op cyberincidenten, gaan vaker uit van een vertrouwensband tussen de dienstverlener en de afnemer.
- De partijen die zich goed of volledig gezamenlijk voorbereiden op cyberincidenten zijn vaker digitaal veilige afnemers.

Onderlinge cybersecurity afstemming niet volledig afgestemd?

- IT-dienstverleners denken cybersecurity concreter afgestemd te hebben met hun afnemers dan dat de afnemers het denken afgestemd te hebben met hun IT-dienstverlener(s).

CONCLUSIE

motivaction
insights and strategy

Cyberverantwoordelijkheden: Gedeelde verantwoordelijkheid is...

IT-dienstverleners en IT-afnemers vinden dat ze gedeelde verantwoordelijkheid hebben voor de digitale veiligheid van IT-afnemers

- IT-dienstverleners dichten zichzelf een grotere rol toe bij de digitale veiligheid van IT-afnemers, dan dat de IT-afnemers dat doen; want IT-dienstverleners vinden minder vaak dat afnemers volledig verantwoordelijk zijn voor hun digitale veiligheid (12% vs. 24%).
- IT-dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de IT-dienstverlener ligt, terwijl IT-afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt.

Verantwoordelijkheid zou meer naar de dienstverlener moeten/kunnen

- Volgens IT-dienstverleners zou de verantwoordelijkheid meer bij de IT-dienstverlener moeten liggen dan nu het geval is. Als we de huidige en gewenste situatie vergelijken, zien we het zwaartepunt van verantwoordelijkheid verschuiven naar de dienstverlenerskant.
- Ook volgens IT-afnemers zou de verantwoordelijkheid wat meer naar de dienstverlener moeten/mogen schuiven dan nu het geval is.

Cyberkennis: Cyberadvies inwinnen

Voor IT-advies ga je naar de IT-specialist

- Voor afnemers is hun IT-dienstverlener de go-to voor advies over cyberveiligheid.
- Voor IT-dienstverleners is de IT Security specialist / Collega IT-dienstverlener het aanspreekpunt voor advies over cyberveiligheid.

IT-dienstverleners weten overheid vaker te vinden voor cyberadvies

- IT-dienstverleners zeggen vaker dan afnemers cyberadvies te zoeken bij het Nationaal Cyber Security Centrum (28% vs. 19%).
- IT-dienstverleners zeggen vaker dan afnemers cyberadvies te zoeken bij het Digital Trust Center (21% vs. 10%).

ADVIEZEN

motivaction
insights and strategy

Advies Cyberveilig Gedrag

Voorkom blinde vlekken door overzicht en tips te bieden

→ Een veelgenoemde reden voor gebrek aan voorbereiding, is het vertrouwen van IT-dienstverleners en IT-afnemers in zichzelf en elkaar. Hoewel vertrouwen erg belangrijk is, kunnen hierdoor wel blinde vlekken ontstaan. De overheid zou hier een rol in kunnen spelen door het opstellen van een checklist van de zaken die afgestemd moeten worden en tips hoe de partijen dit goed kunnen afstemmen.

Advies CyberKennis

Richt de communicatie op de IT-dienstverleners

→ IT-dienstverleners gaan voor advies over cyberveiligheid vaker naar de overheid (DTC en NCSC) dan IT-afnemers. IT-afnemers gaan voor advies juist naar hun dienstverlener. Communicatie over cyberveiligheid vanuit de overheid kan dus het best gericht worden op IT-dienstverleners. Geef daarbij ook tips of versimpelde uitleg die IT-dienstverleners kunnen doorgeven aan hun afnemers.

Advies Cyberveilige houdingen

Help bij het nemen van de juiste maatregelen ter voorbereiding op een cyberincident

→ Veel IT-dienstverleners, en in iets mindere mate IT-afnemers, maken zich zorgen om de digitale veiligheid van het bedrijf van de afnemer. Vertrouwen in de genomen maatregelen kan helpen om deze zorgen te verminderen. Help IT-dienstverleners en IT-afnemers bij het nemen van de juiste maatregelen. Dit kan de overheid doen door aan te geven welke maatregelen belangrijk zijn bij bepaalde dreigingen. Hierbij kunnen IT-dienstverleners en IT-afnemers gericht kijken hoe goed zij voorbereid zijn op specifieke dreigingen en hoe zij zich nog beter kunnen voorbereiden.

SAMENVATTING

motivaction
insights and strategy

Resultaten CyberKennis

Afnemers gaan vooral naar hun dienstverlener voor advies; dienstverleners gaan vooral naar een IT security aanbieder of collega dienstverleners

- Zes op de tien (63%) afnemers zouden naar hun dienstverlener gaan als ze advies willen over IT security/digitale veiligheid. Dienstverleners zoeken vooral advies bij een IT security aanbieder (45%) en collega IT-dienstverleners (35%).

Dienstverleners en afnemers geven elkaar voornamelijk tips over goede afspraken en communicatie

- Wanneer gevraagd wordt welke tips dienstverleners en afnemers elkaar zouden geven, dan gaan de meeste antwoorden over goede afspraken en communicatie. Zo noemen ze het maken van duidelijke/goede afspraken (dienstverleners: 15%, afnemers: 12%), transparantie (dienstverleners: 7%, afnemers: 5%) en heldere communicatie/uitleg (dienstverleners: 3%, afnemers: 12%).

Resultaten Cyberveilige houdingen

Dienstverleners maken zich meer zorgen om de digitale veiligheid van hun klanten dan afnemers zich zorgen maken om hun eigen bedrijf

- Acht op de tien (79%) dienstverleners maken zich (zeer veel) zorgen om de digitale veiligheid van hun klanten. Zes op de tien (60%) afnemers maken zich (zeer veel) zorgen om de digitale veiligheid van hun bedrijf.
  - Vertrouwen in elkaar is de voornaamste reden voor afnemers en dienstverleners om zich geen of weinig zorgen te maken om digitale veiligheid. Zo geeft 64% van dienstverleners en 43% van afnemers aan te vertrouwen op (de maatregelen getroffen door) de dienstverlener. Daarnaast geeft 36% van dienstverleners en 46% van afnemers aan te vertrouwen op (de maatregelen getroffen door) de afnemer.
  - De ervaren impact van een cyberincident is de grootste reden om wel zorgen te maken om digitale veiligheid: 42% van dienstverleners en 48% van afnemers geeft dit als reden voor hun zorgen.

SAMENVATTING

motivaction
insights and strategy

Resultaten Cyberveilig Gedrag

Een meerderheid heeft ervaring met cyberincidenten

- Een meerderheid geeft aan weleens te maken te hebben gehad met cyberincidenten. Zo geeft twee derde aan weleens phishing mails te hebben ontvangen (dienstverleners: 68%, afnemers: 67%). Verder geeft ruim de helft van dienstverleners (55%) en vier tiende van afnemers (37%) aan te maken te hebben gehad met verstuurde phishing mails uit naam van het bedrijf waar ze werken.

Hoewel een relatief groot deel van dienstverleners en afnemers aangeeft matig tot niet voorbereid te zijn op cyberincidenten, hebben de meesten wel al stappen gezet in de voorbereiding

- Twee op de tien dienstverleners (18%) geven aan dat zij matig tot niet voorbereid zijn op cyberincidenten samen met hun klanten. Drie op de tien afnemers (30%) geven aan dat hun bedrijf matig tot niet voorbereid is op een cyberincident. Wanneer gevraagd wordt naar de concrete mate van voorbereiding zien we dit aandeel toenemen: 44% van afnemers geeft hier aan matig tot niet voorbereid te zijn. Onder dienstverleners blijft dit aandeel vrijwel gelijk (20%).
  - Vertrouwen in de (diensten van) de dienstverlener en een kleine ervaren kans op incidenten zijn de meest genoemde redenen om niet of matig voor te bereiden op cyberincidenten: vier op de tien afnemers (resp. 39% en 40%) en twee op de tien dienstverleners (resp. 20% en 18%) noemen deze redenen.
- Bijna alle dienstverleners (95%) en afnemers (96%) geven aan minimaal één maatregel te hebben getroffen om een kans op en/of de impact van een cyberincident te verminderen. Onder dienstverleners is een firewall voor alle systemen verbonden met internet de meest getroffen maatregel (46%). Onder afnemers is dit antivirus software (64%).
- Een meerderheid geeft aan in enige mate concreet te hebben gesproken over cyberdreigingen met hun dienstverlener/afnemer. Zo geeft driekwart aan vaste contactpersonen te hebben (dienstverleners: 77%, afnemers: 74%). Echter geven zes op de tien aan dat ze werken op basis van vertrouwen en te denken dat het vast ook goed komt in geval van een cyberincident (dienstverleners: 62%, afnemers: 59%).

SAMENVATTING

motivaction
insights and strategy

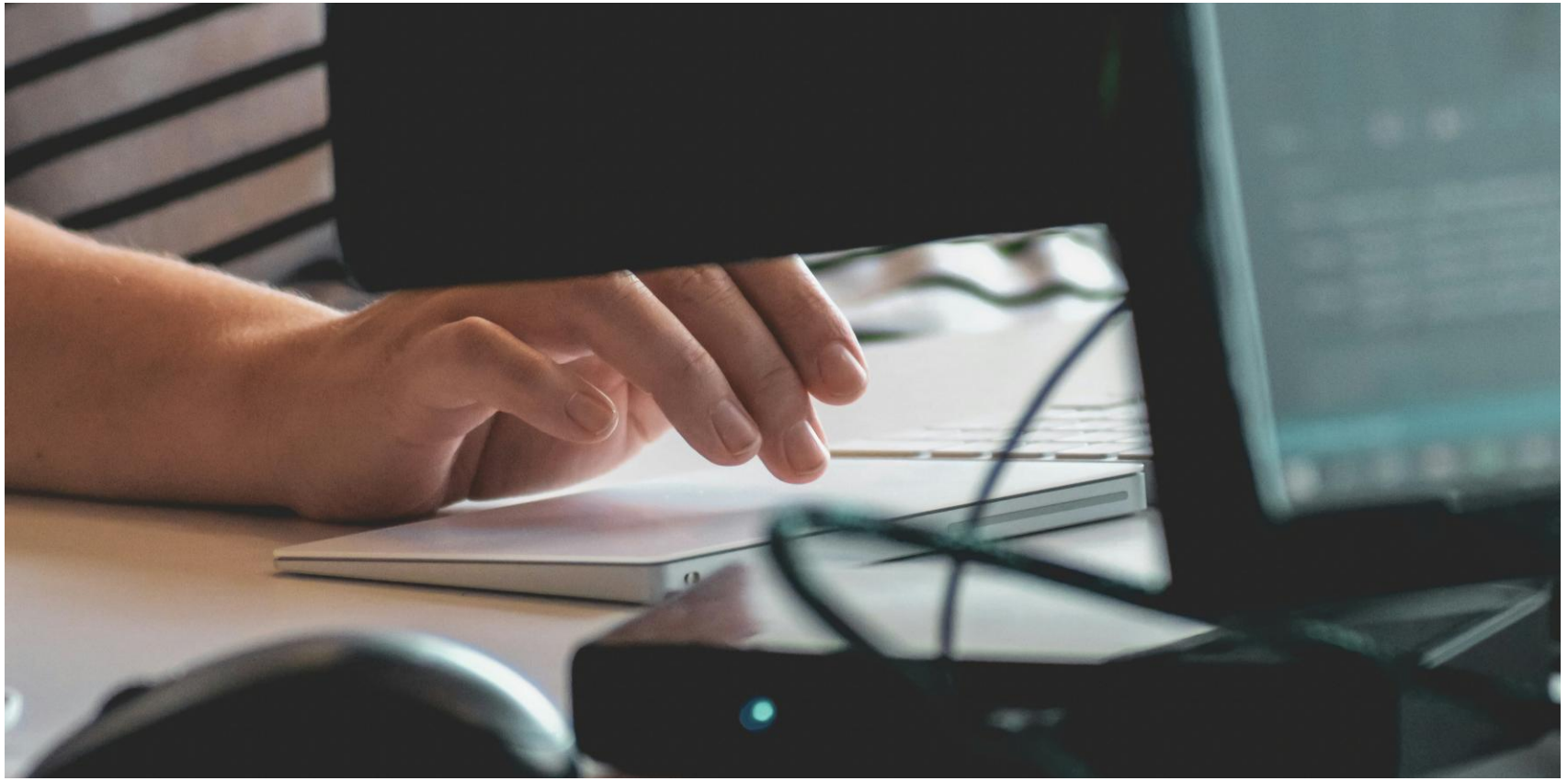
Resultaten Cyberverantwoordelijkheden

Afnemers en dienstverleners vinden dat ze gedeelde verantwoordelijkheid moeten hebben voor de digitale veiligheid van het bedrijf van de afnemer

- Ruim vier op de tien vinden dat de afnemer en de dienstverlener gedeelde verantwoordelijkheid hebben voor de digitale veiligheid van het bedrijf van de afnemer (dienstverleners: 44%, afnemers: 43%). Circa een kwart vindt dat beide verantwoordelijk zijn, maar dat de afnemer meer verantwoordelijkheid draagt (dienstverlener: 26%, afnemer: 22%). Circa een tiende vindt juist dat de dienstverlener meer verantwoordelijkheid draagt (dienstverlener: 13%, afnemer: 9%).
- Ook als het specifiek gaat om Security Services vinden afnemers en dienstverleners van Security Services dat zij gedeelde verantwoordelijkheid hebben (dienstverleners: 41%, afnemers: 42%).
- Wanneer gevraagd wordt waar de dienstverlener precies verantwoordelijk moet zijn, geven zowel afnemers als dienstverleners voornamelijk aan dat de dienstverlener verantwoordelijk is voor de digitale veiligheid op het gebied van de services die zij leveren.

Dienstverleners zeggen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt en zou moeten liggen, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt en zou moeten liggen.

- Waar de verantwoordelijkheid ligt, verschilt per maatregel. Voor sommige maatregelen ligt de verantwoordelijkheid meer bij de dienstverlener. Dit geldt bijvoorbeeld voor patchen, voor actieve monitoring en detectie en voor netwerk segmentatie. Bij andere maatregelen, zoals training van medewerkers en het afsluiten van een cyberverzekering, ligt de verantwoordelijkheid meer bij de afnemer.
  - Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid meer bij hen ligt dan bij de afnemer.
- Ook de gewenste verantwoordelijkheid verschilt per maatregel. Deze gewenste verantwoordelijkheid komt grotendeels overeen met de daadwerkelijke verantwoordelijkheid. Zo zou de verantwoordelijkheid voor patchen, actieve monitoring en detectie en netwerk segmentatie meer bij de dienstverlener moeten liggen dan bij de afnemer en zou de verantwoordelijkheid voor training van medewerkers en het afsluiten van een cyberverzekering meer bij de afnemer moeten liggen.
  - Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid meer bij hen zou moeten liggen dan bij de afnemer.



Resultaten Cyberveilig gedrag:

Gedrag t.a.v. digitale veiligheid van de eigen organisatie en dat van de zakelijke partner

Meerderheid heeft ervaring met één of meer cyberincidenten; Dienstverleners hebben meer ervaring met cyberincidenten dan afnemers

Dienstverleners geven bij bijna alle cyberincidenten vaker aan er ervaring mee te hebben dan afnemers.

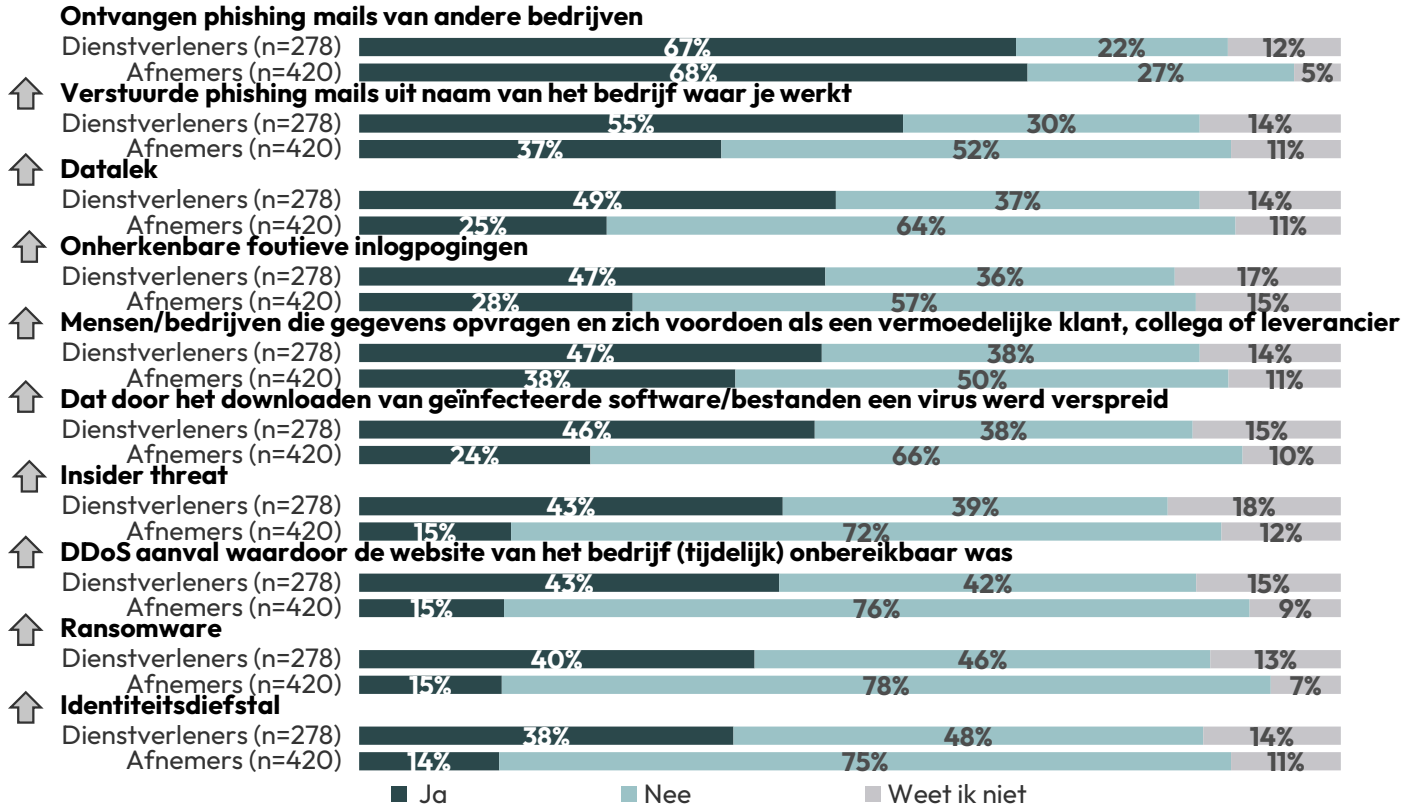
Digitaal veilige afnemers geven vaker aan weleens te maken te hebben gehad met een DDOS aanval (23% vs. 15% van alle afnemers), verstuurde phishing mails (45% vs. 37%), ontvangen phishing mails (76% vs. 68%) en een datalek (34% vs. 25%).

Praktisch digitale afnemers geven minder vaak aan ervaring te hebben met een datalek (16% vs. 25%), onherkenbare foutieve inlogpogingen (19% vs. 28%) en insider threat (9% vs. 15%).

Digitaal waakzame afnemers geven vaker aan ervaring te hebben met onherkenbare foutieve inlogpogingen (37% vs. 28%).

⇧ = vaker 'ja' beantwoord door dienstverleners dan door afnemers
⇩ = minder vaak 'ja' beantwoord door dienstverleners dan door afnemers

Afnemers: Heeft het bedrijf waar je werkt weleens te maken gehad met de onderstaande cyberincidenten?
Dienstverleners: Voor zover je dat weet, hebben de bedrijven waar jullie IT-diensten voor leveren weleens te maken gehad met de onderstaande cyberincidenten? (Basis – allen)



Klik hier voor de tabellen.

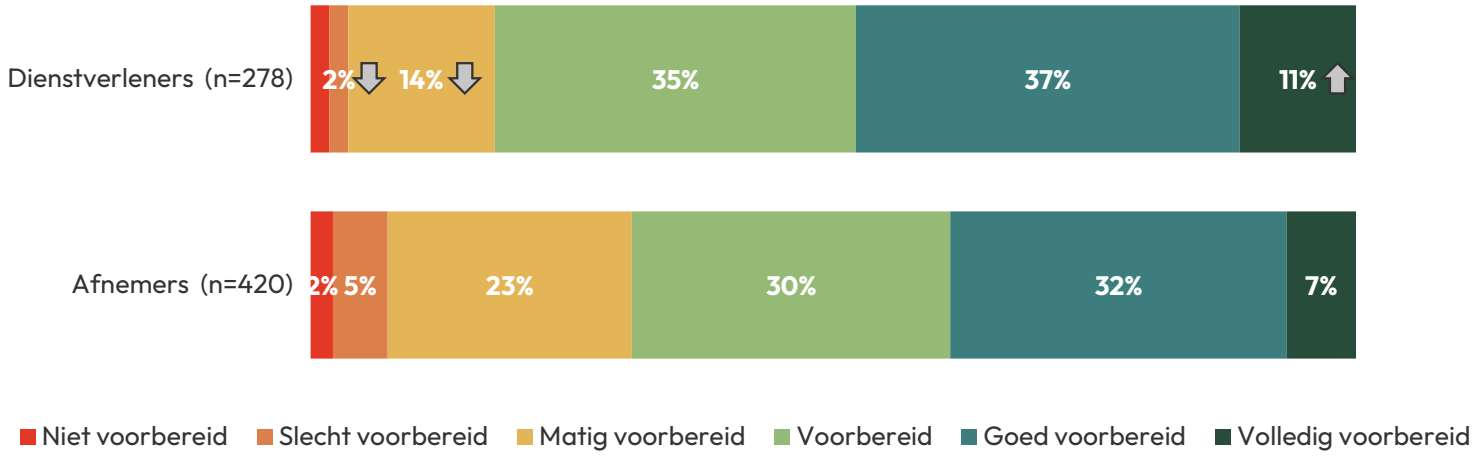
Cyberveilig gedrag: voorbereidingen

Dienstverleners schatten hun mate van voorbereiding op een cyberincident hoger in dan afnemers

Dienstverleners zeggen vaker dat zij en hun klanten volledig voorbereid zijn op cyberincidenten dan afnemers (11% vs. 7%)

Afnemers: Wanneer het gaat om een cyberincident waardoor netwerken, systemen en data meer dan 24 uur niet bereikbaar zijn in hoeverre is het bedrijf voorbereid op deze situatie?
Dienstverleners: Wanneer het gaat om een cyberincident waardoor netwerken, systemen en data meer dan 24 uur niet bereikbaar zijn in hoeverre hebben de meeste bedrijven, waar jullie IT-diensten aan leveren, zich voorbereid op deze situatie samen met jullie? (Basis – allen)

Digitaal veilige afnemers geven vaker aan goed (52% vs. 32%) of volledig (13% vs. 7%) voorbereid te zijn.
Terwijl **praktisch digitale afnemers** vaker aangeven matig voorbereid te zijn (36% vs. 23%).



= vaker genoemd door dienstverleners dan door afnemers
= minder vaak genoemd door dienstverleners dan door afnemers

Cyberveilig gedrag: Cyberreadiness afgestemd

Dienstverleners geven vaker aan concreet voorbereid te zijn op een cyberincident dan afnemers

Ook de concrete mate van voorbereiding wordt hoger geschat door dienstverleners dan door afnemers. Ze zeggen vaker dat ze een plan op hoofdlijnen hebben (goed voorbereid: 37% vs. 26%) of dat ze vaste afspraken hebben (voorbereid: 27% vs. 15%). Dienstverleners zeggen minder vaak dan afnemers dat ze alles op hoofdlijnen hebben besproken (matig voorbereid: 7% vs. 14%) of dat ze het wel eens hebben besproken (slecht voorbereid: 8% vs. 21%).

Digitaal veilige afnemers geven vaker aan goed (37% vs. 26%) of volledig (24% vs. 16%) voorbereid te zijn.
Praktisch digitale afnemers geven vaker aan slecht (38% vs. 21%) of niet (17% vs. 9%) voorbereid te zijn.

Afnemers: Hoe concreet hebben jullie afgestemd hoe er gehandeld wordt in het geval van een cyberincident?
Dienstverleners: Hoe concreet hebben jullie met de meeste bedrijven waar jullie IT-diensten aan leveren afgestemd hoe er gehandeld wordt in het geval van een cyberincident? (Basis – allen)

= vaker genoemd door dienstverleners dan door afnemers
= minder vaak genoemd door dienstverleners dan door afnemers

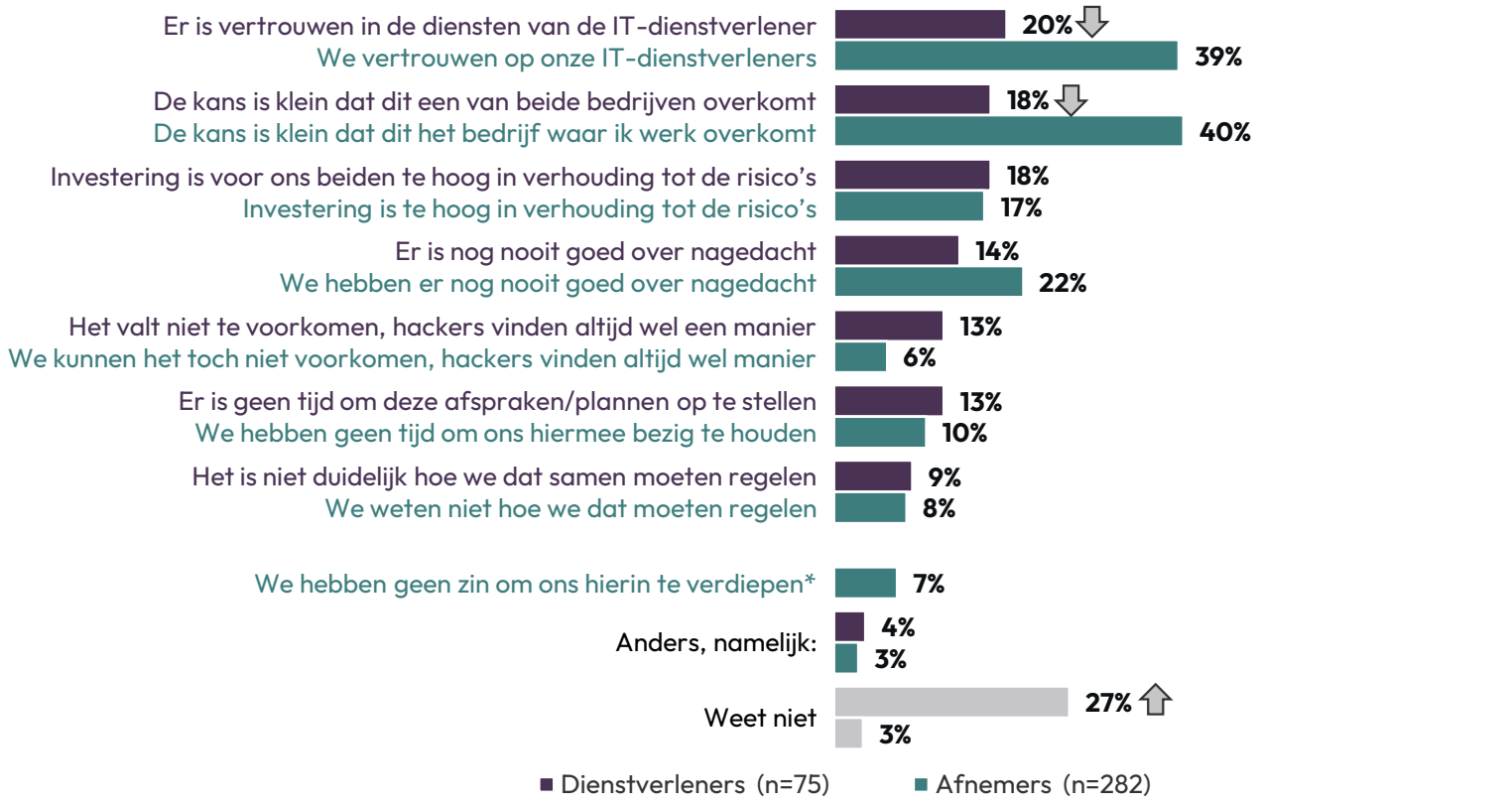
Cyberveilig gedrag: Cyberreadiness niet afgestemd

Vertrouwen in (de diensten van) de dienstverlener en kleine ervaren kans op incidenten zijn redenen voor afnemers en dienstverleners om zich niet of matig voor te bereiden;

Dienstverleners die zich nog niet of matig hebben voorbereid noemen minder vaak vertrouwen in de diensten (20% vs. 39%) of een kleine ervaren kans op incidenten (18% vs. 40%) als reden voor de matige voorbereiding dan afnemers die zich nog niet of matig hebben voorbereid op cyberincidenten.

Afnemers/Dienstverleners: Wat zijn de belangrijkste redenen dat er (nog) geen vaste afspraken/plannen zijn gemaakt ter voorbereiding op een cyberincident?

(Basis – heeft (nog) geen vaste afspraken/plannen gemaakt ter voorbereiding op een cyberincident)



Deze antwoordoptie is alleen voorgelegd aan afnemers

*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

⇧ = vaker genoemd door dienstverleners dan door afnemers

⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Cyberveilig gedrag: Cyberreadines maatregelen

Firewall, antivirus software, automatische back-up en verplicht gebruik van sterke wachtwoorden zijn de meest gebruikte manieren om voor te bereiden op cyberincidenten

Dienstverleners geven vaker dan afnemers dat ze zich hebben voorbereid op een cyberincident door:

- actieve monitoring en detectie (36% vs. 26%),
- encryptie/versleuteling van belangrijke data (35% vs. 28%),
- hardening (27% vs. 20%),
- ingeschreven te zijn op bronnen over kwetsbaarheden en veiligheid (18% vs. 12%), en
- security.txt of hoe ze omgaan met responsible disclosure-meldingen online vindbaar te maken (15% vs. 7%)

Ze geven minder vaak dan afnemers aan voor te bereiden door:

- antivirus software (42% vs. 64%),
- automatische back-up van systemen (42% vs. 53%),
- verplicht gebruik van sterke wachtwoorden (40% vs. 50%)

Digitaal veilige afnemers geven bij bijna alle maatregelen vaker aan ze getroffen te hebben, terwijl **praktisch digitale afnemers** dit juist minder vaak zeggen

⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Afnemers/Dienstverleners: Op welke manier(en) is het bedrijf waar je werkt voorbereid om een kans op en/of de impact van een cyberincident te verminderen? (Basis – allen)	**Afnemers (n=420)**	**Dienstverleners (n=278)**
Firewall voor alle systemen verbonden met internet	51%	46%
Antivirus software	64%	42% ⇩
Automatische back-up van systemen	53%	42% ⇩
Verplicht gebruik sterke wachtwoorden	50%	40% ⇩
Multifactor authenticatie voor toegang tot belangrijkste systemen	41%	38%
Beveiligde internetverbindingen (bijvoorbeeld standaard afgedwongen HTTPS)	38%	38%
Security specialist(en) zijn beschikbaar (intern of extern)	36%	36%
Actieve monitoring en detectie	26%	36% ⇧
Encryptie/versleuteling van belangrijke data	28%	35% ⇧
Vergroting bewustzijn medewerkers (door training)	38%	33%
Rechten voor toegang tot gevoelige data worden weloverwogen toegekend	38%	33%
Er is een risico-analyse uitgevoerd waarna passende maatregelen zijn getroffen	26%	31%
Bedrijfsbreed uitrollen beveiligingsupdates indien beschikbaar ('patchen')	28%	30%
Draaiboek opgesteld hoe te handelen bij een cyberincident	27%	29%
Rechten voor toegang tot gevoelige data zijn altijd up-to-date	29%	28%
Functionaliteit beperken of uitschakelen waar deze onnodig is of een te groot risico vormt ('hardening')	20%	27% ⇧
Netwerk segmentatie om dreiging in het gehele netwerk te voorkomen	20%	26%
Ingeschreven op bronnen over kwetsbaarheden en veiligheid	12%	18% ⇧
Security.txt of hoe we omgaan met responsible disclosure-meldingen is online vindbaar	7%	15% ⇧
Cyberverzekering afgesloten	12%	13%
Geen maatregelen getroffen	4%	5%

Cyberveilig gedrag: Cyberreadiness afgestemd

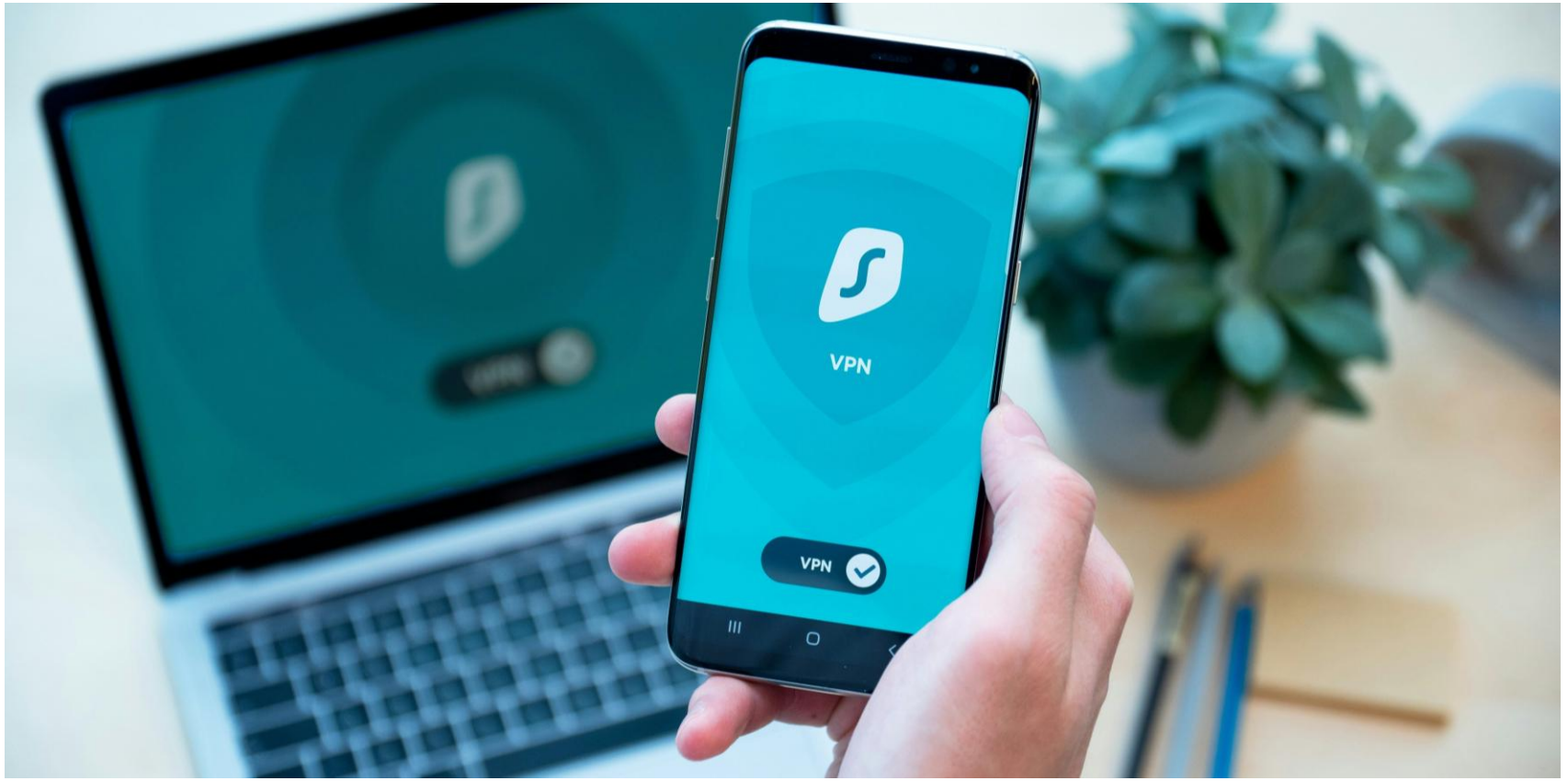
Dienstverleners geven aan cybersecurity concreter afgestemd te hebben met hun klanten dan afnemers met hun dienstverlener(s)

Dienstverleners geven vaker aan dat zij en hun klanten werken volgens afspraken opgenomen in het contract/de SLA (76% vs. 62%). Daarnaast geven ze vaker dan afnemers aan dat zij en hun klanten gezamenlijk de risico's hebben vastgesteld (73% vs. 59%) en dat ze een gezamenlijk draaiboek hebben klaarliggen (72% vs. 53%). Ook geven dienstverleners vaker aan dat zij en hun klanten regelmatig het gezamenlijk draaiboek testen/oefenen (69% vs. 43%).

Digitaal veilige afnemers geven aan de cybersecurity concreter afgestemd te hebben met hun dienstverlener(s) dan andere afnemers. Zo geven ze vaker aan een gezamenlijk draaiboek te hebben (72% vs. 53%), te werken volgens afspraken opgenomen in het contract/SLA (77% vs. 62%), regelmatig het draaiboek te testen (58% vs. 43%) en vaste contactpersonen te hebben (42% vs. 74%).
Praktisch digitale afnemers geven dit minder vaak aan (resp. 32%, 43%, 25% en 62%).

Afnemers: Kan jij aangeven in hoeverre je het eens bent met de volgende stellingen met betrekking tot het bedrijf waar je werkt, in relatie tot IT-dienstverleners?
Dienstverleners: Kan jij aangeven in hoeverre je het eens bent met de volgende stellingen met betrekking tot het bedrijf waar je werkt, in relatie tot IT-afnemers? (Basis – allen)

= Dienstverleners zijn gemiddeld meer eens met stelling dan afnemers
= Dienstverleners zijn gemiddeld minder eens met stelling dan afnemers



Resultaten Cyberveilige houdingen:

Mate van zorgen t.a.v. cyberincidenten en cybercriminaliteit

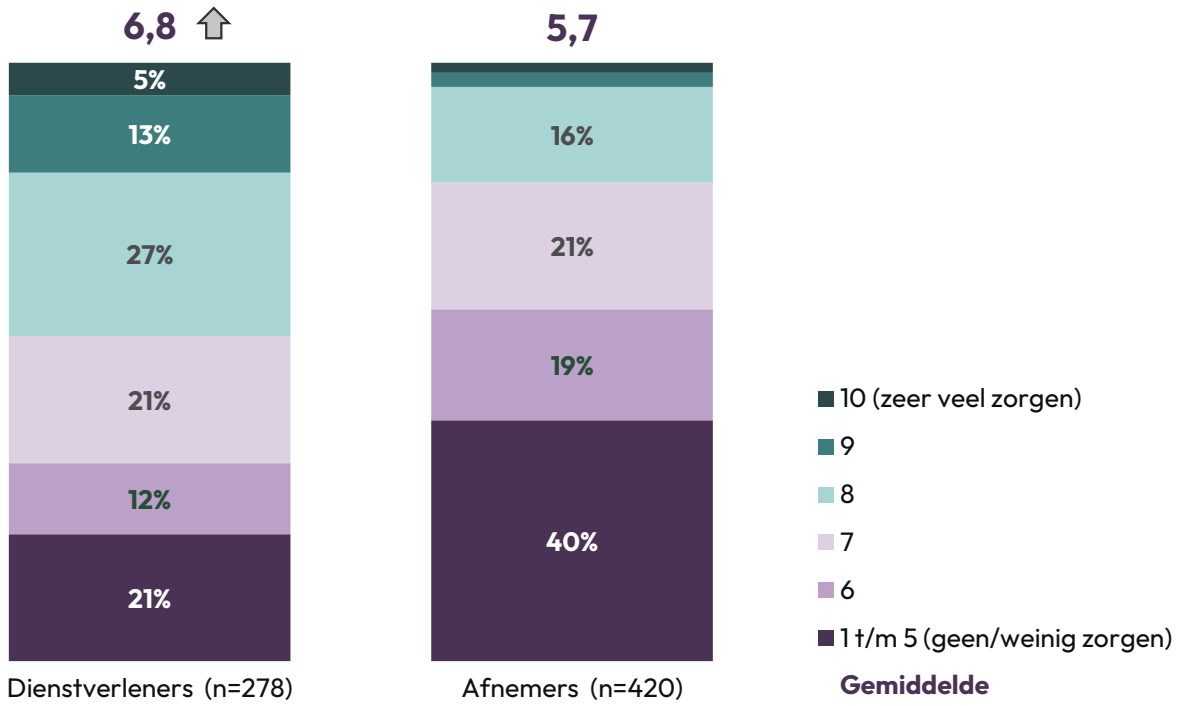
Cyberveilige houdingen: Zorgen

Dienstverleners maken zich meer zorgen om de digitale veiligheid van hun klanten dan afnemers zich zorgen maken om hun eigen bedrijf

Dienstverleners maken zich gemiddeld meer zorgen om de digitale veiligheid van hun klanten dan afnemers zich zorgen maken om hun eigen bedrijf (6,8 vs. 5,7).

Digitaal veilige afnemers (5,3 vs. 5,7) en **praktisch digitale afnemers** (5,2 vs. 5,7) maken zich gemiddeld minder zorgen om de digitale veiligheid van hun bedrijf.
Digitaal waakzame afnemers maken zich hier meer zorgen om (6,5 vs. 5,7).

Afnemers: In hoeverre maak je je zorgen over de digitale veiligheid (cybersecurity) van het bedrijf waar je werkt?
Dienstverleners: In hoeverre maak jij je over het algemeen zorgen over de digitale veiligheid (cybersecurity) van de bedrijven waar jullie IT-diensten aan leveren? (Basis – allen)



= hoger onder dienstverleners dan onder afnemers
= lager onder dienstverleners dan onder afnemers

Cyberveilige houdingen: Geen zorgen

Vertrouwen in elkaar is de voornaamste reden voor afnemers en dienstverleners om zich geen of weinig zorgen te maken om digitale veiligheid

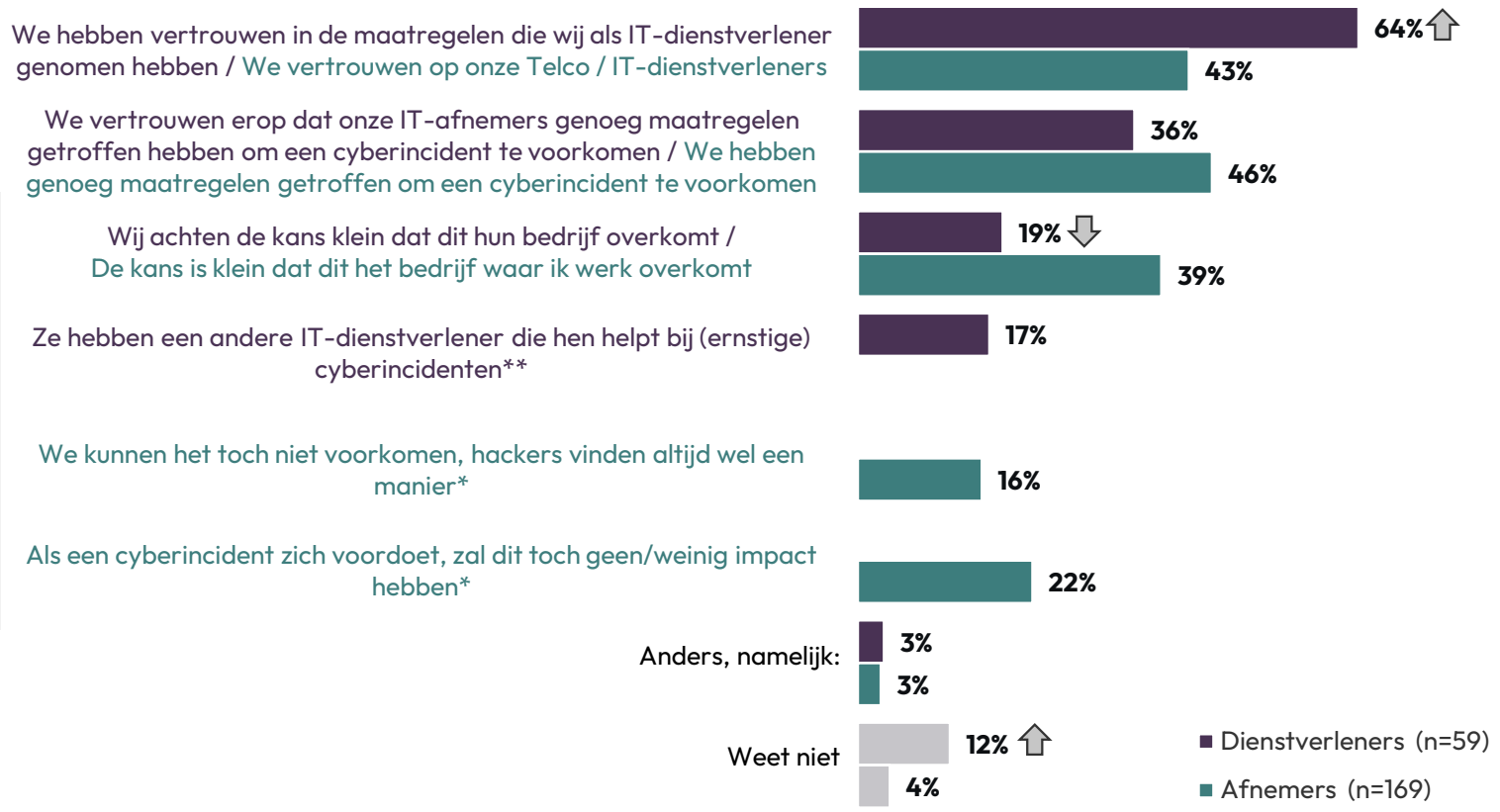
Dienstverleners geven vaker aan zich geen of weinig zorgen te maken omdat ze vertrouwen hebben in de maatregelen die zij als dienstverlener hebben genomen (64% vs. 43%). Ze geven aan minder vaak te denken dat de kans klein is dat dit hun bedrijf overkomt (19% vs. 39%).

Digitaal veilige afnemers die zich weinig zorgen maken, geven vaker als reden dat ze genoeg maatregelen hebben getroffen om een cyberincident te voorkomen (67% vs. 46%). **Praktisch digitale afnemers** die zich weinig zorgen maken, geven vaker als reden dat ze denken dat de kans klein is dat dit hun bedrijf overkomt (63% vs. 39%) en dat een cyberincident toch weinig impact zal hebben (35% vs. 22%).

**Deze antwoordoptie is alleen voorgelegd aan afnemers*
*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Afnemers: Wat is de belangrijkste reden dat het bedrijf waar je werkt zich geen of weinig zorgen maakt om digitale veiligheid?
Dienstverleners: Wat is de belangrijkste reden dat jij je geen of weinig zorgen maakt om de digitale veiligheid van de bedrijven waar jullie IT-diensten aan leveren? (Basis – maakt zich geen tot weinig zorgen)



Cyberveilige houdingen: Zorgen

Impact van een cyberincident is de voornaamste reden voor zorgen om digitale veiligheid

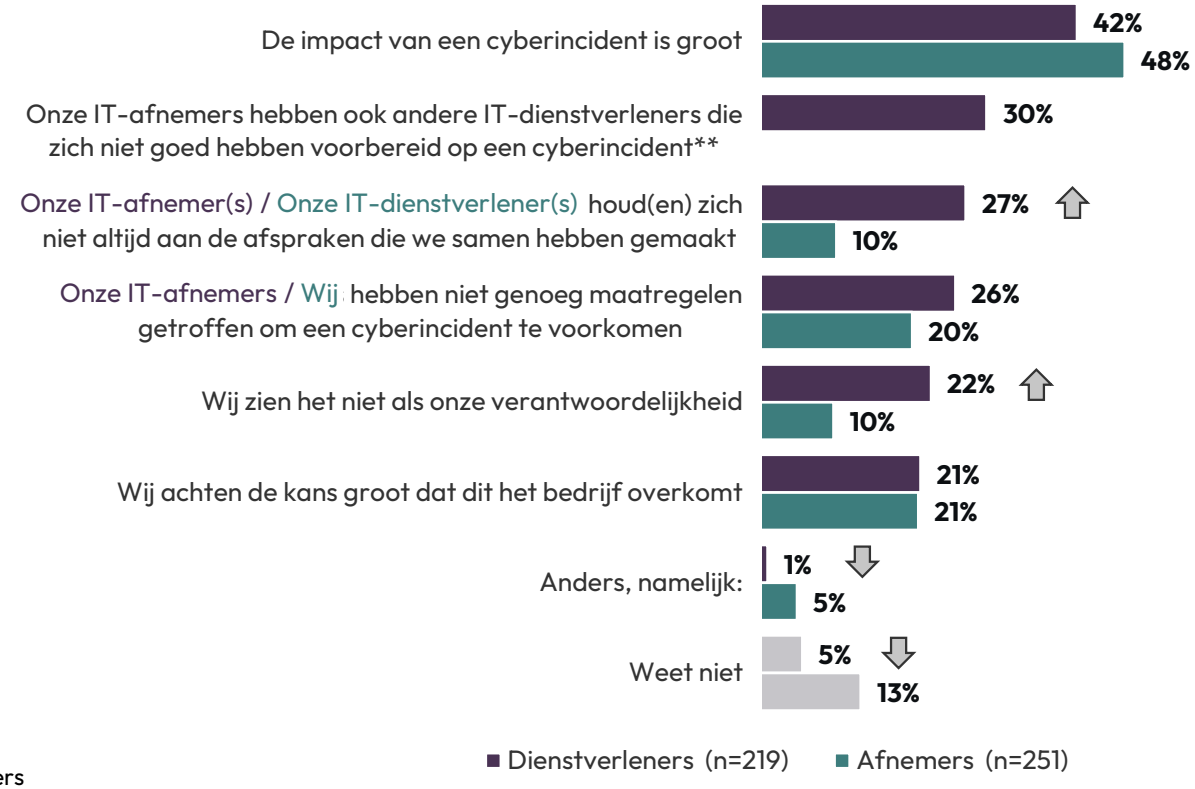
Dienstverleners maken zich vaker dan afnemers zorgen om de digitale veiligheid, omdat ze denken dat hun klanten zich niet altijd aan de afspraken houden (27% vs. 10%) of omdat ze het niet zien als hun verantwoordelijkheid (22% vs. 10%).

Digitaal waakzame afnemers die zich (veel) zorgen maken, geven vaker als reden hiervoor dat de impact van een cyberincident groot is (61% vs. 48%).

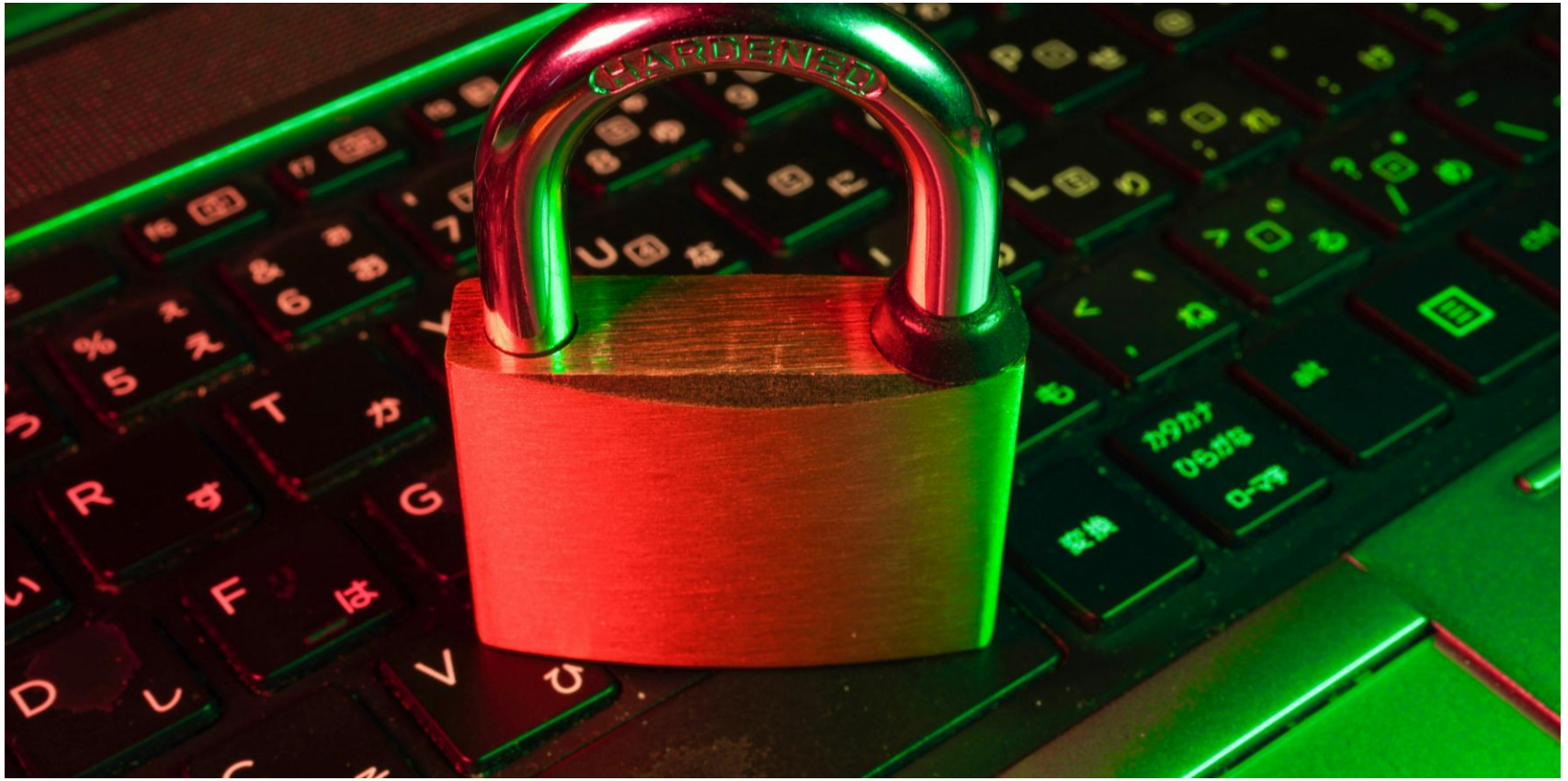
**Deze antwoordoptie is alleen voorgelegd aan afnemers*
*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Afnemers: Wat is de belangrijkste reden dat jij je (veel) zorgen maakt om de digitale veiligheid van het bedrijf?
Dienstverleners: Wat is de belangrijkste reden dat jij je (veel) zorgen maakt om de digitale veiligheid van de bedrijven waar jullie IT-diensten aan leveren? (Basis – maakt zich (veel) zorgen)



motivaction
insights and strategy



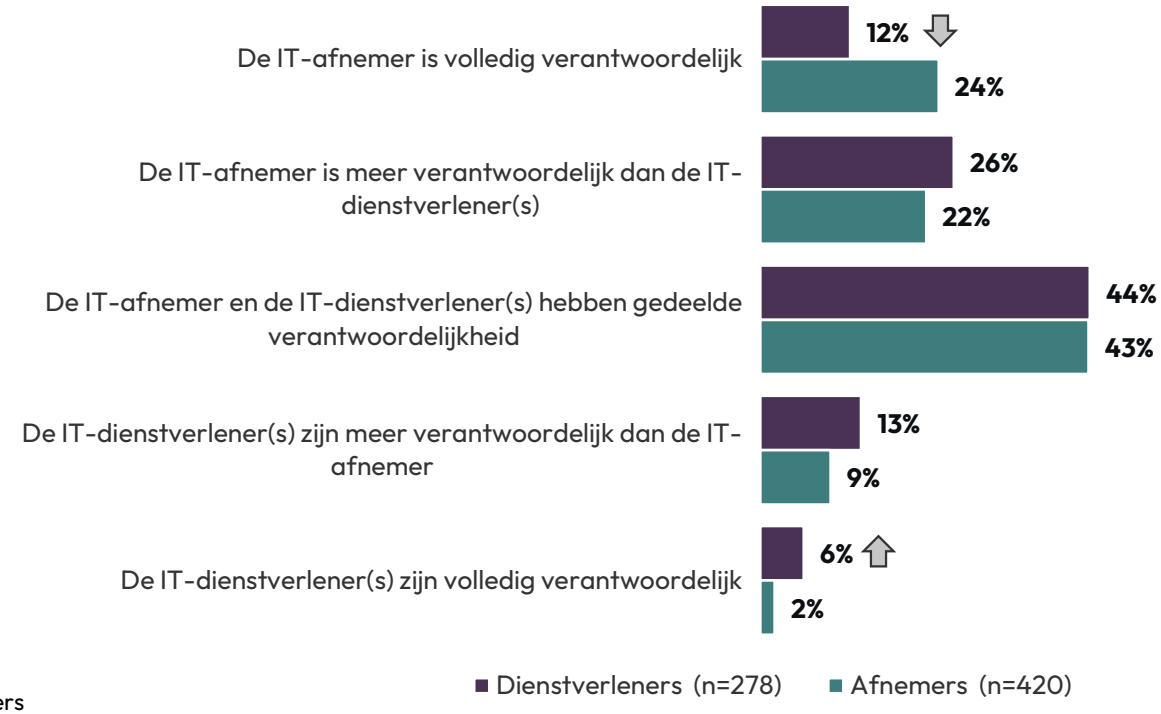
Resultaten Cyberverantwoordelijkheden:

Cyberveiligheid verwachtingen tussen IT-afnemers en IT-dienstverleners

Afnemers en dienstverleners vinden dat ze gedeelde verantwoordelijkheid hebben voor digitale veiligheid

Dienstverleners vinden minder vaak dat afnemers volledig verantwoordelijk zijn voor hun digitale veiligheid (12% vs. 24%).

Afnemers: Kun je aangeven in welke mate jij vindt dat het bedrijf zelf en/of de IT-dienstverlener(s) verantwoordelijk zijn voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je aangeven in welke mate jij vindt dat jullie (het IT-bedrijf waar jij werkt) en/of de IT-afnemer verantwoordelijk zijn voor de digitale veiligheid van hun bedrijf? (Basis – allen)



= vaker genoemd door dienstverleners dan door afnemers
= minder vaak genoemd door dienstverleners dan door afnemers

Klik hier voor de tabellen.

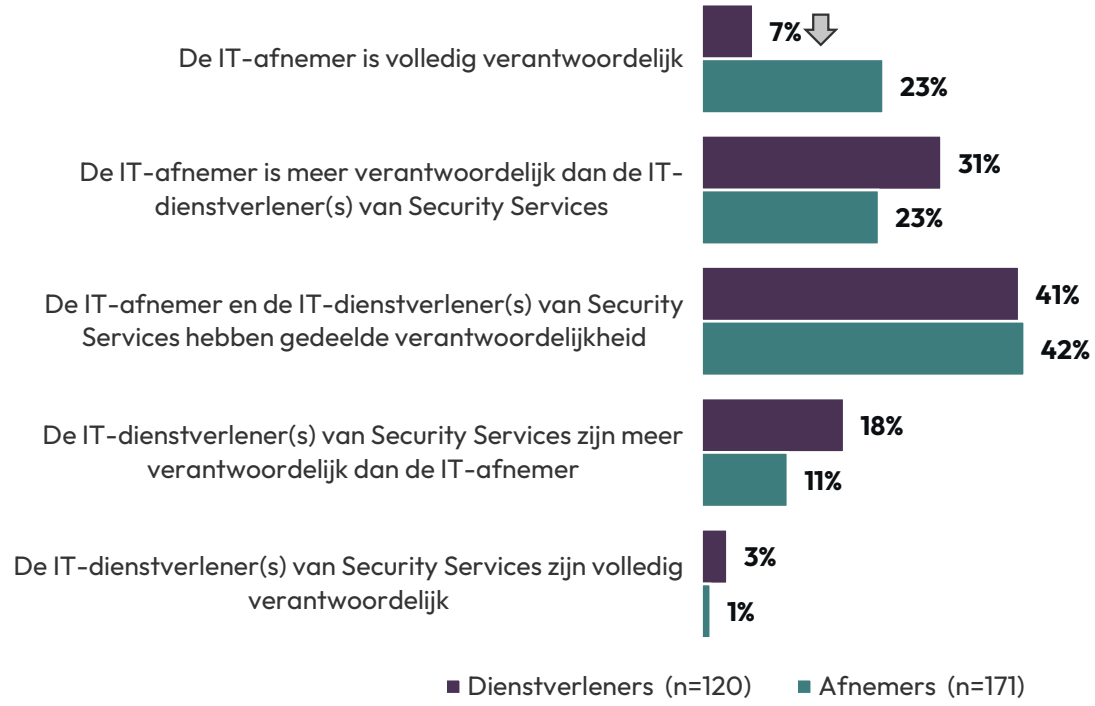
Cyberverantwoordelijkheden: Security services

Afnemers en dienstverleners van Security Services vinden dat ze gedeelde verantwoordelijkheid hebben voor digitale veiligheid

Dienstverleners vinden minder vaak dat de afnemer volledig verantwoordelijk is (7% vs. 23%) dan afnemers.

Digitaal veilige afnemers achten zichzelf vaker volledig verantwoordelijk (38% vs. 23%) dan andere afnemers.

Afnemers: Kun je aangeven in welke mate jij vindt dat het bedrijf zelf en/of de IT-dienstverlener(s) van Security Services verantwoordelijk zijn voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je aangeven in welke mate jij vindt dat jullie (het IT-bedrijf waar jij werkt) en/of de IT-afnemer van Security Services verantwoordelijk zijn voor de digitale veiligheid van hun bedrijf?
(Basis – neemt security services af/levert security services)



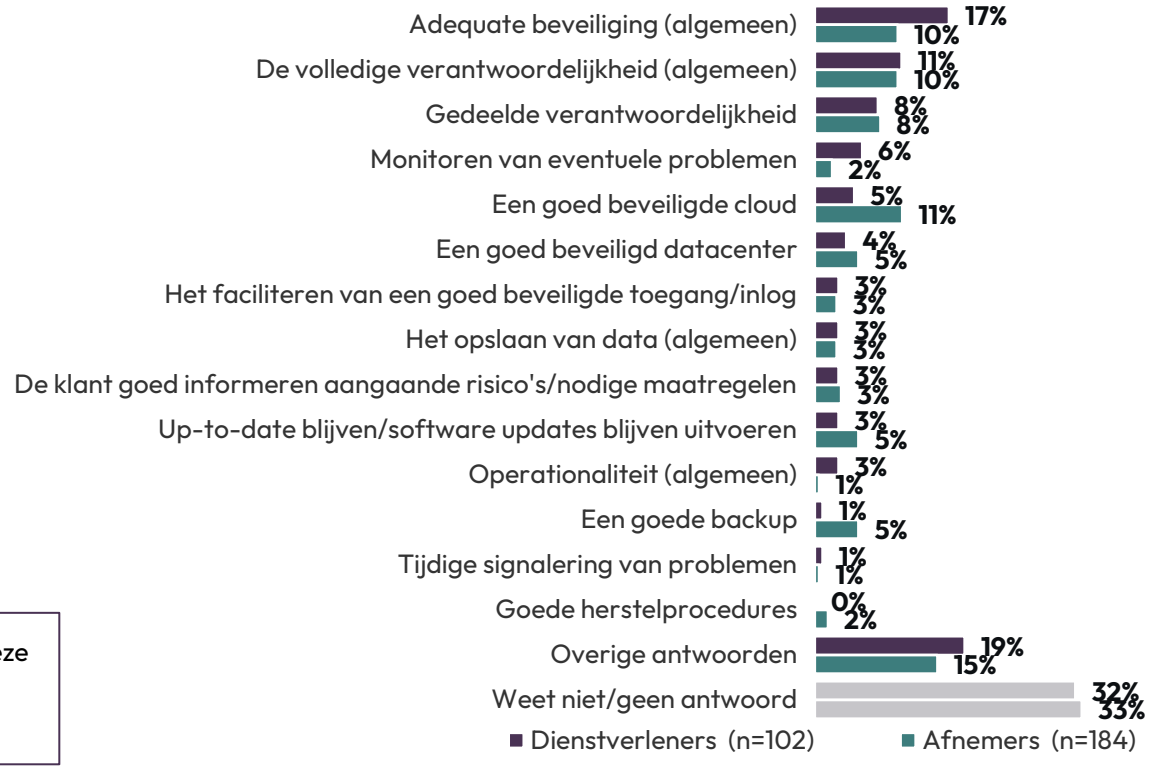
⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Cyberverantwoordelijkheden: Cloud & datacenter services

Dienstverleners van Cloud & Datacenter Services worden voornamelijk verantwoordelijk geacht voor de beveiliging van de cloud en het datacenter; een tiende geeft aan dat dienstverleners volledig verantwoordelijk zijn

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat de IT-dienstverlener(s) van Cloud & Datacenter Services hebben voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat jullie als IT-dienstverlener van Cloud & Datacenter Services hebben voor de digitale veiligheid van het bedrijf waar jullie deze dienst aan leveren?
(Basis – neemt Cloud & Datacenter Services af/levert Cloud & Datacenter Services)



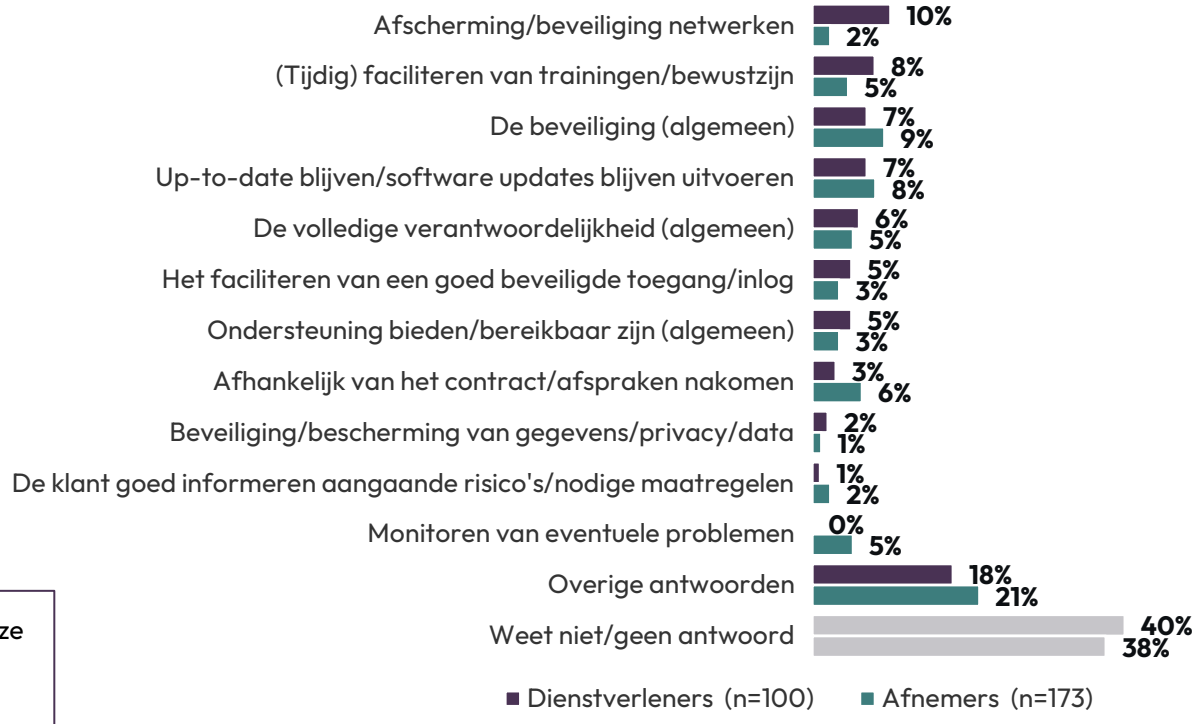
Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

Cyberverantwoordelijkheden: Werkplek & end-user services

Dienstverleners van Werkplek & End-user Services worden vooral verantwoordelijk gehouden voor netwerkbeveiliging en het faciliteren van trainingen

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat de IT-dienstverlener(s) van Werkplek & End-user Services hebben voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat jullie als IT-dienstverlener van Werkplek & End-user Services hebben voor de digitale veiligheid van het bedrijf waar jullie deze dienst aan leveren?
(Basis – neemt Werkplek & End-user Services af/levert Werkplek & End-user Services)



Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

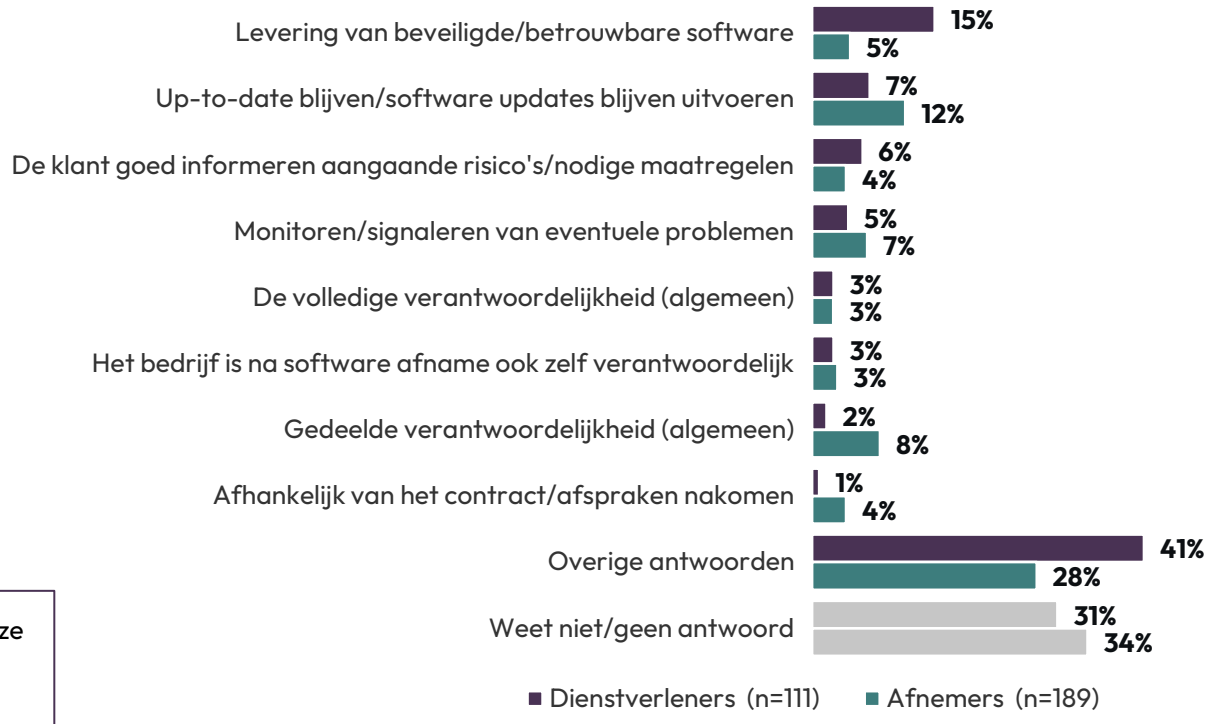
Klik hier voor de tabellen.
Klik om de definitie van de IT-diensten te bekijken.

Cyberverantwoordelijkheden: Software services

Dienstverleners van Software Services worden vooral verantwoordelijk gehouden voor het leveren en up-to-date houden van beveiligde software en het informeren van klanten over risico's

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat de IT-dienstverlener(s) van Software Services hebben voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat jullie als IT-dienstverlener van Software Services hebben voor de digitale veiligheid van het bedrijf waar jullie deze dienst aan leveren?
(Basis – neemt Software Services af/levert Software Services)



Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

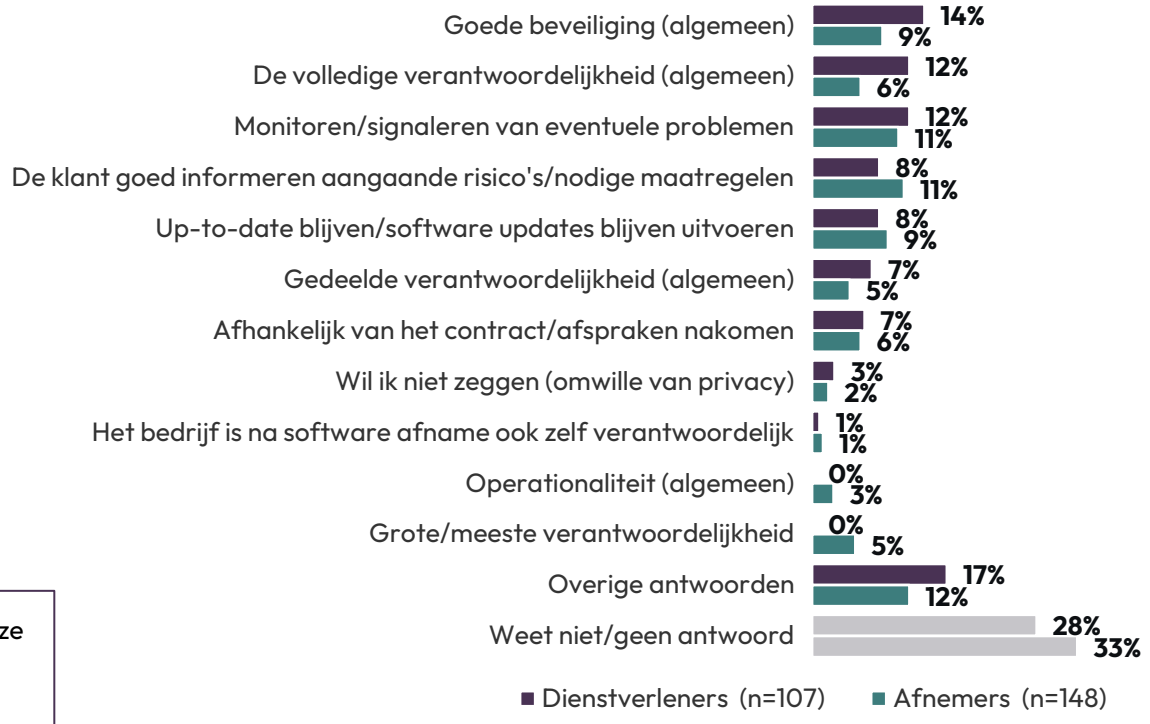
Klik hier voor de tabellen.
Klik om de definitie van de IT-diensten te bekijken.

Cyberverantwoordelijkheden: Security services

Dienstverleners van Security Services worden vooral verantwoordelijk gehouden voor goede beveiliging en het monitoren van problemen; een tiende geeft aan dat dienstverleners volledig verantwoordelijk zijn

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat de IT-dienstverlener(s) van Security Services hebben voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat jullie als IT-dienstverlener van Security Services hebben voor de digitale veiligheid van het bedrijf waar jullie deze dienst aan leveren?
(Basis – neemt Security Services af/levert Security Services)



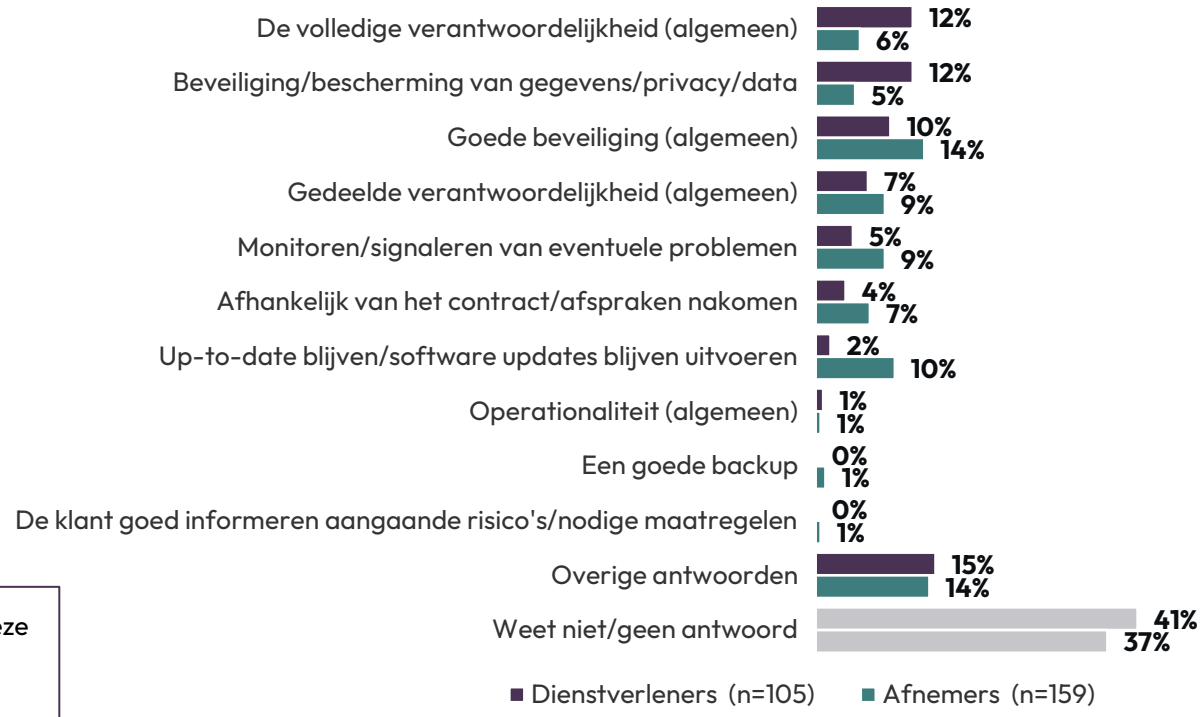
Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

Cyberverantwoordelijkheden: Platform & data services

Dienstverleners van Platform & Data Services worden vooral verantwoordelijk gehouden voor goede beveiliging van data; een tiende geeft aan dat dienstverleners volledig verantwoordelijk zijn

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat de IT-dienstverlener(s) van Platform & Data Services hebben voor de digitale veiligheid van het bedrijf?
Dienstverleners: Kun je zo volledig mogelijk aangeven welke verantwoordelijkheid jij vindt dat jullie als IT-dienstverlener van Platform & Data Services hebben voor de digitale veiligheid van het bedrijf waar jullie deze dienst aan leveren?
(Basis – neemt Platform & Data Services af/levert Platform & Data Services)



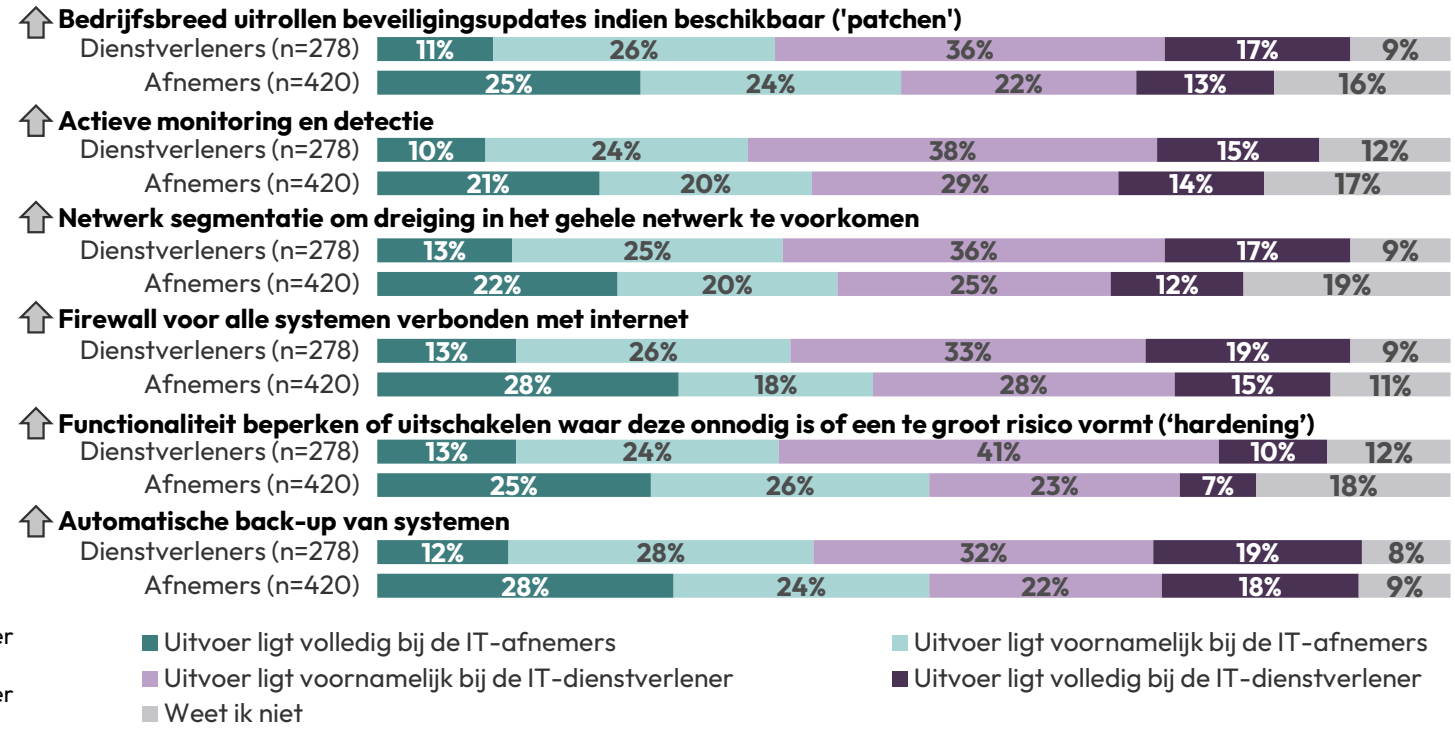
Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

Klik hier voor de tabellen.
Klik om de definitie van de IT-diensten te bekijken.

Dienstverleners zeggen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt.

Afnemers: Kun je voor de volgende maatregelen aangeven hoe het nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe het doorgaans nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
(Basis – allen)



⇧ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-dienstverleners dan volgens IT-afnemers
⇩ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-afnemers dan volgens IT-afnemers

Klik hier voor de tabellen.

Cyberverantwoordelijkheden: huidige executie

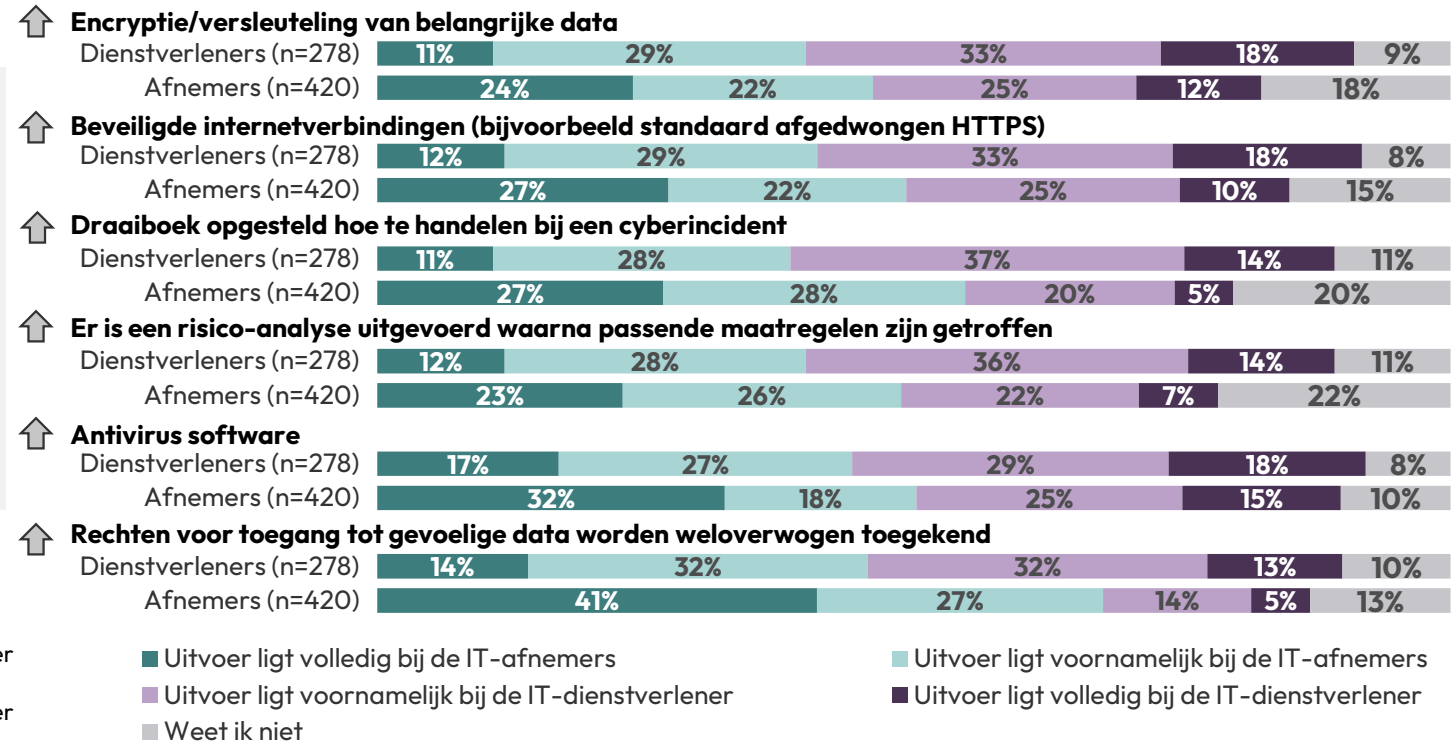
Dienstverleners zeggen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt.

Digitaal veilige afnemers geven vaker aan dat de verantwoordelijkheid voor het opstellen van een draaiboek (65% vs. 55%) en het uitvoeren van een risico-analyse (59% vs. 49%) (voornamelijk) bij hen ligt.

Praktisch digitale afnemers geven juist vaker aan dat de verantwoordelijkheid voor het uitvoeren van een risico-analyse (voornamelijk) bij de dienstverlener ligt (36% vs. 30%).

Afnemers: Kun je voor de volgende maatregelen aangeven hoe het nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe het doorgaans nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
(Basis – allen)



⇧ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-dienstverleners dan volgens IT-afnemers
⇩ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-afnemers dan volgens IT-afnemers

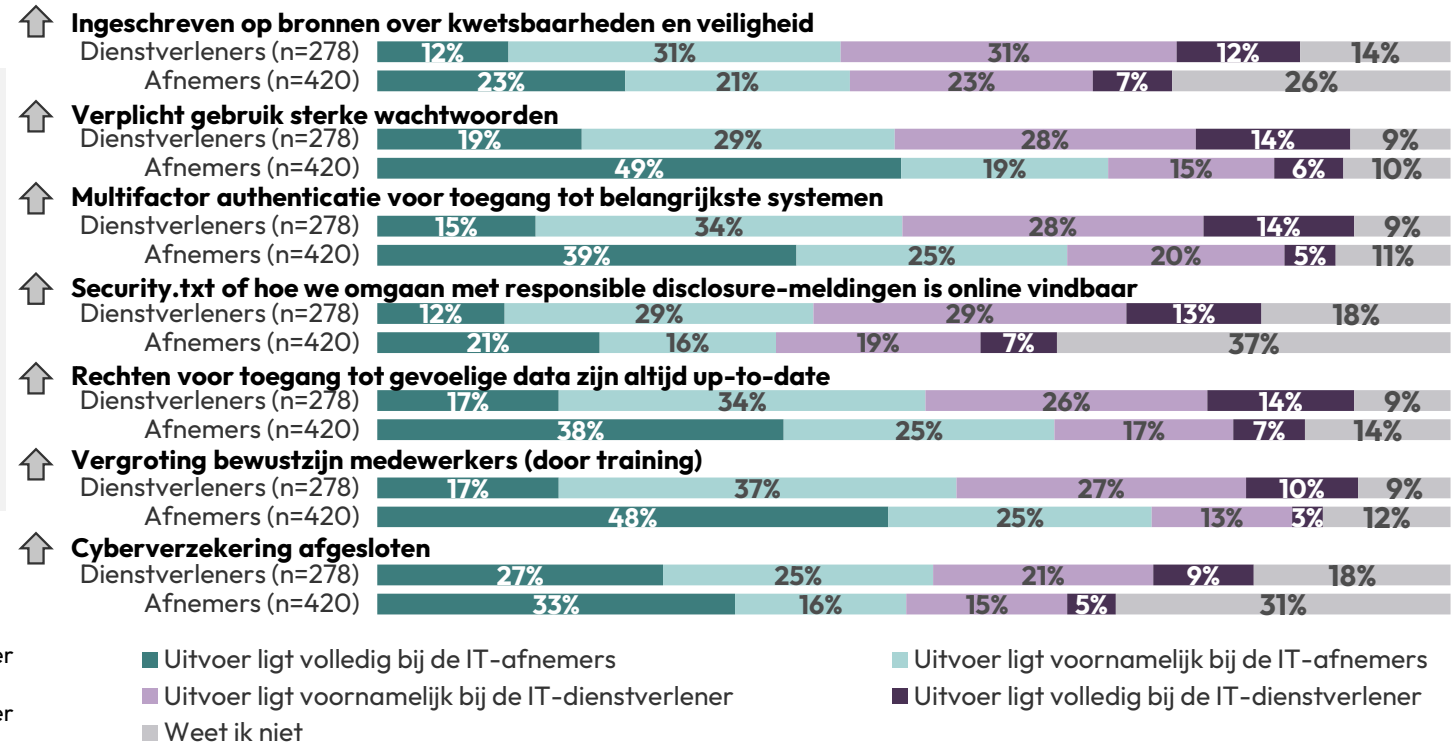
Cyberverantwoordelijkheden: huidige executie

Dienstverleners zeggen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener ligt, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen ligt.

Praktisch digitale afnemers geven vaker aan dat de verantwoordelijkheid voor het online vindbaar maken van security.txt (voornamelijk) bij de dienstverlener ligt (32% vs. 26%).

Afnemers: Kun je voor de volgende maatregelen aangeven hoe het nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe het doorgaans nu geregeld is; Bij wie ligt, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen?
(Basis – allen)



⇧ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-dienstverleners dan volgens IT-afnemers
⇩ = verantwoordelijkheid ligt volgens de IT-dienstverleners meer bij de IT-afnemers dan volgens IT-afnemers

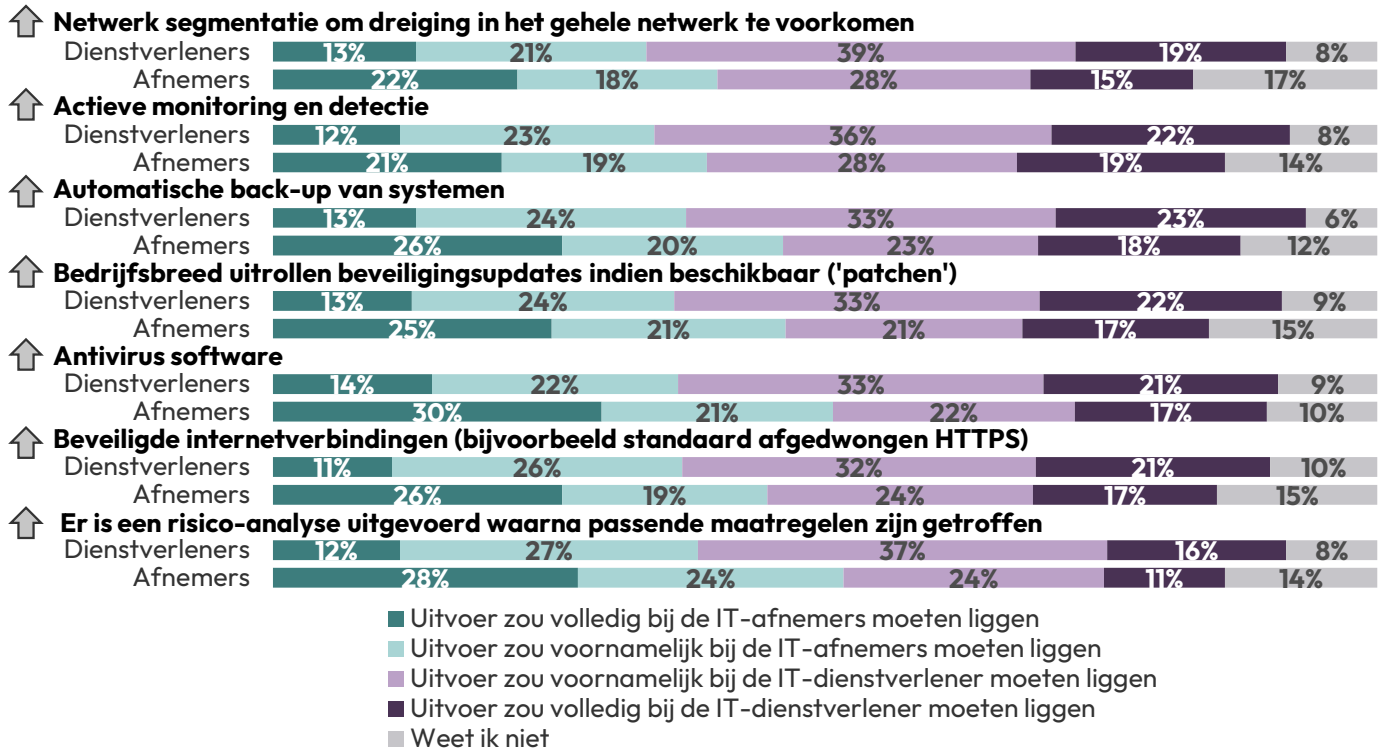
Cyberverantwoordelijkheden: gewenste executie

Geen eenduidig beeld over gewenste verantwoordelijkheid; dienstverleners vinden vaker dat het bij hen zou moeten liggen, terwijl afnemers vinden dat het bij de afnemer moet liggen

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener zou moeten liggen, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen zou moeten liggen.

Praktisch digitale afnemers vinden vaker dat de verantwoordelijkheid voor automatische back-up van systemen (voornamelijk) bij de dienstverlener zou moeten liggen (48% vs. 41%). Daarnaast vinden ze vaker dat dienstverleners (voornamelijk) verantwoordelijk zouden moeten zijn voor het uitvoeren van een risico-analyse (42% vs. 35%) en actieve monitoring/detectie (55% vs. 47%).

Afnemers: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
(Basis – allen)



⇧ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-dienstverleners moeten liggen dan volgens IT-afnemers
⇩ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-afnemers moeten liggen dan volgens IT-afnemers

Cyberverantwoordelijkheden: gewenste executie

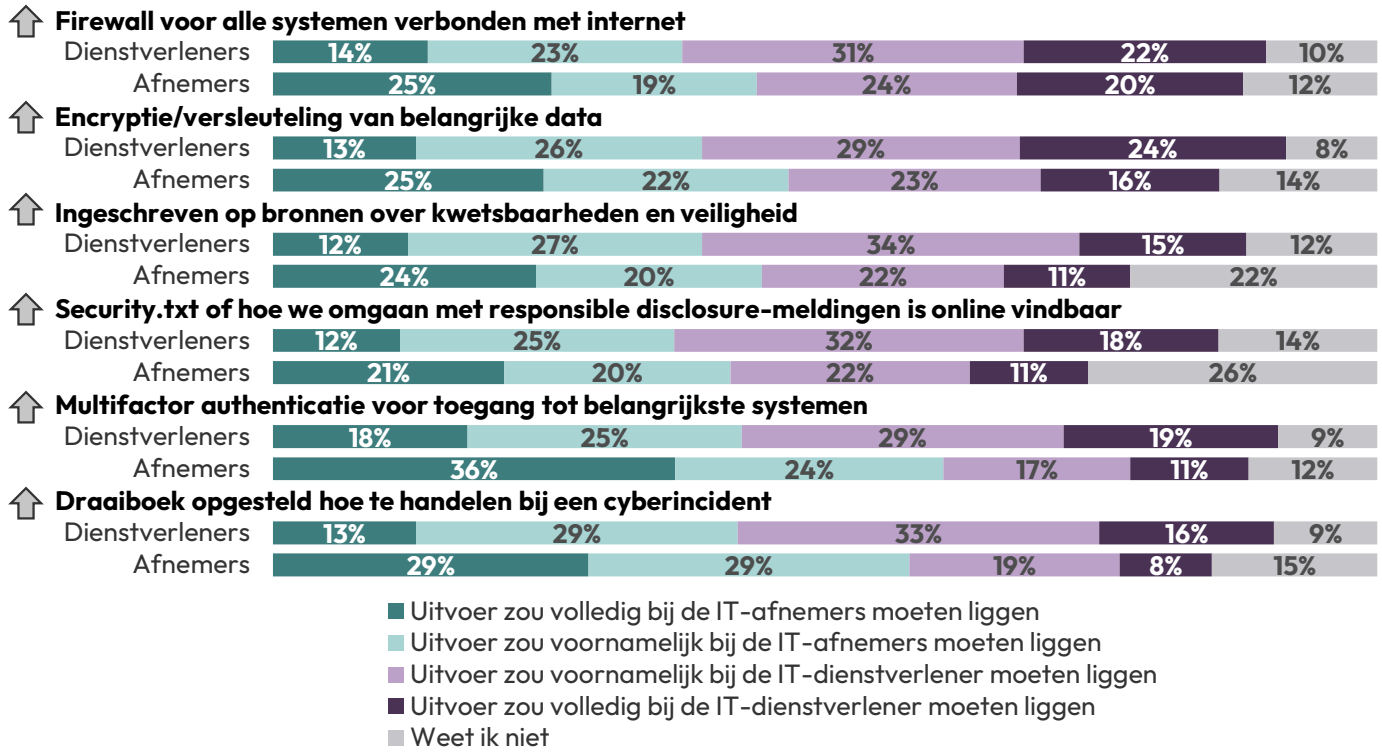
Geen eenduidig beeld over gewenste verantwoordelijkheid; dienstverleners vinden vaker dat het bij hen zou moeten liggen, terwijl afnemers vinden dat het bij de afnemer moet liggen

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener zou moeten liggen, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen zou moeten liggen.

Praktisch digitale afnemers vinden vaker dat de verantwoordelijkheid voor encryptie van belangrijke data (voornamelijk) bij de dienstverlener zou moeten liggen (48% vs. 39%).

Digitaal veilige afnemers vinden juist vaker dat deze verantwoordelijkheid (voornamelijk) bij hen zou moeten liggen (56% vs. 47%).

Afnemers: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
(Basis – allen)



⇧ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-dienstverleners moeten liggen dan volgens IT-afnemers
⇩ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-afnemers moeten liggen dan volgens IT-afnemers

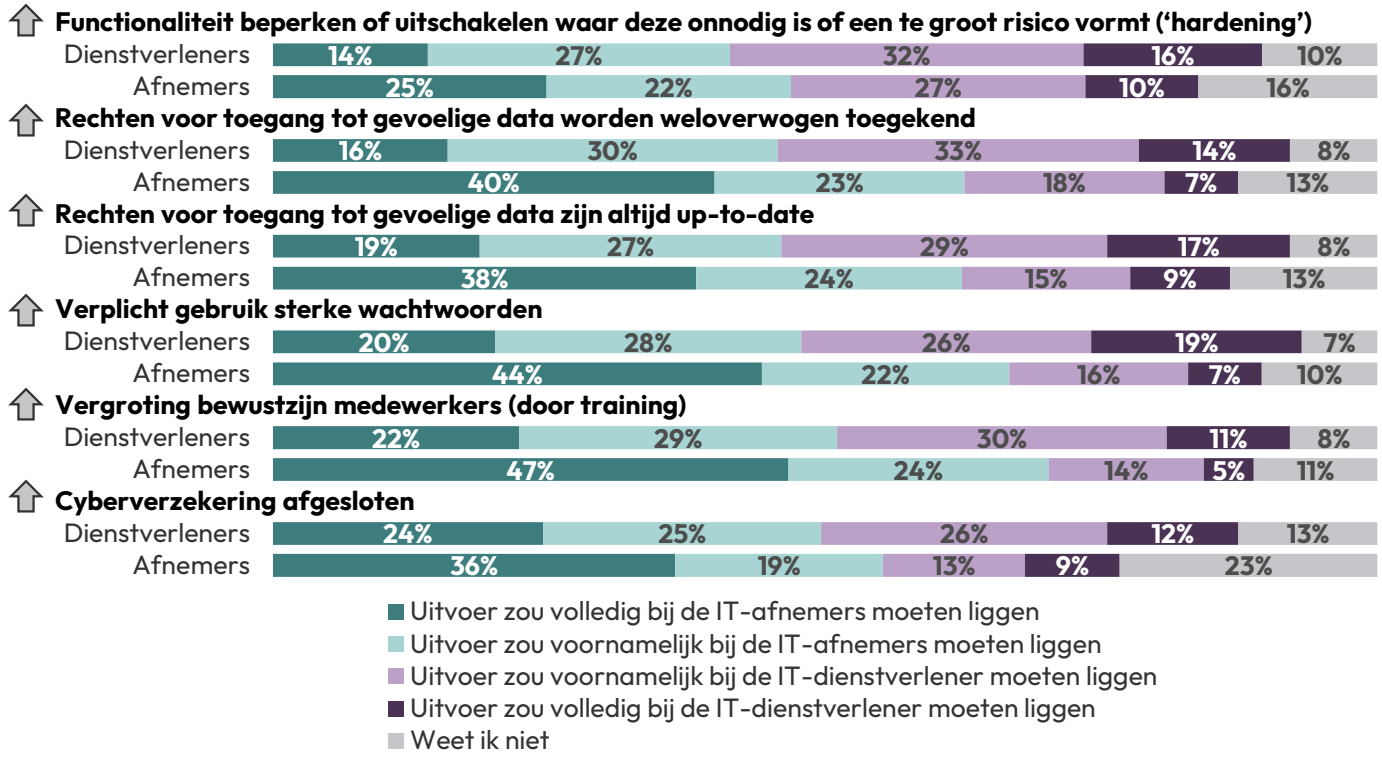
Cyberverantwoordelijkheden: gewenste executie

Geen eenduidig beeld over gewenste verantwoordelijkheid; dienstverleners vinden vaker dat het bij hen zou moeten liggen, terwijl afnemers vinden dat het bij de afnemer moet liggen

Dienstverleners zeggen bij alle maatregelen vaker dat de verantwoordelijkheid (voornamelijk) bij de dienstverlener zou moeten liggen, terwijl afnemers vaker zeggen dat de verantwoordelijkheid bij hen zou moeten liggen.

Praktisch digitale afnemers vinden vaker dat de verantwoordelijkheid voor het up-to-date houden van rechten (voornamelijk) bij de dienstverlener zou moeten liggen (33% vs. 24%). Daarnaast vinden ze vaker dat dienstverleners (voornamelijk) verantwoordelijk zouden moeten zijn voor hardening (49% vs. 37%).

Afnemers: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
Dienstverleners: Kun je voor de volgende maatregelen aangeven hoe jij vindt dat het geregeld moet zijn; Bij wie zou, volgens jou, primair de verantwoordelijkheid voor de uitvoering van deze maatregelen moeten liggen?
(Basis – allen)



⇧ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-dienstverleners moeten liggen dan volgens IT-afnemers
⇩ = verantwoordelijkheid zou volgens de IT-dienstverleners meer bij de IT-afnemers moeten liggen dan volgens IT-afnemers

Verantwoordelijkheid zou meer naar de dienstverlener moeten

Volgens dienstverleners zou de verantwoordelijkheid meer bij de dienstverlener moeten liggen dan nu het geval is. Als we de huidige en gewenste situatie vergelijken, zien we over het algemeen het zwaartepunt van verantwoordelijkheid verschuiven naar de dienstverlenerskant:

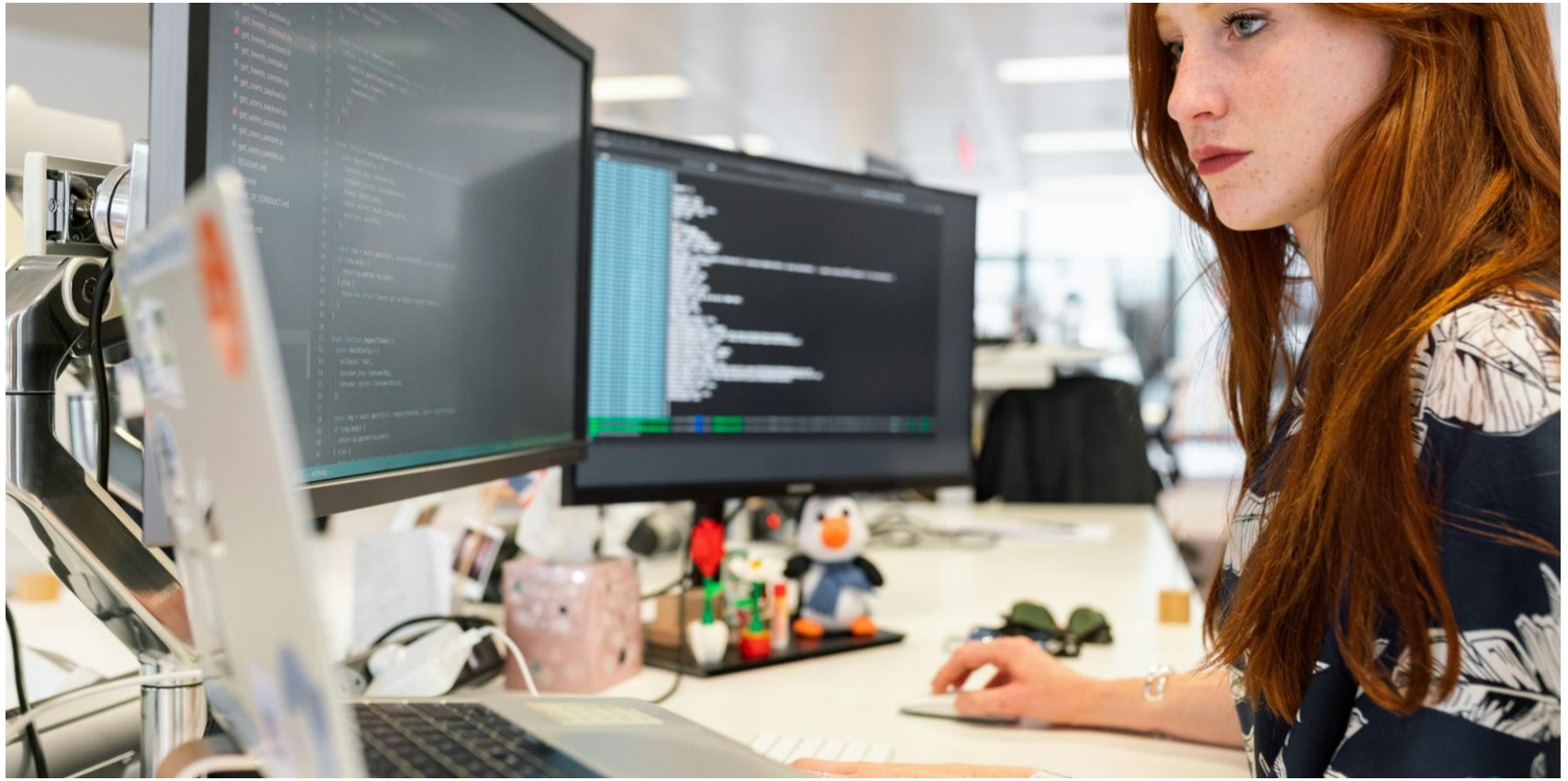
- Antivirus software: 27% van dienstverleners geeft aan dat de verantwoordelijkheid hiervoor momenteel voornamelijk bij de afnemer ligt, terwijl 22% zegt dat de verantwoordelijkheid voornamelijk bij de afnemer zou moeten liggen
- Verplicht gebruik sterke wachtwoorden: 14% geeft aan dat de verantwoordelijkheid momenteel volledig bij de dienstverlener ligt, terwijl 19% zou willen dat de verantwoordelijkheid volledig bij de dienstverlener ligt.
- Multifactor authenticatie: 34% zegt dat de verantwoordelijkheid voornamelijk bij de afnemer ligt, terwijl 25% zegt dat de verantwoordelijkheid voornamelijk bij de afnemer zou moeten liggen. Daarnaast zegt 14% dat de verantwoordelijkheid nu volledig bij de dienstverlener ligt, terwijl 19% wil dat de verantwoordelijkheid volledig bij de dienstverlener ligt.
- Patchen: 17% zegt dat de volledige verantwoordelijkheid bij de dienstverlener ligt, terwijl 22% wil dat de volledige verantwoordelijkheid bij de dienstverlener ligt.
- Rechten up-to-date houden: 34% geeft aan dat de verantwoordelijkheid voornamelijk bij de afnemer ligt, terwijl 27% wil dat de verantwoordelijkheid voornamelijk bij de afnemer ligt.
- Encryptie: 18% geeft aan dat de verantwoordelijkheid hiervoor volledig bij de dienstverlener ligt, terwijl 24% wil dat de verantwoordelijkheid volledig bij de dienstverlener ligt.
- Hardening: 10% zegt dat de verantwoordelijkheid volledig bij de dienstverlener ligt, terwijl volgens 16% de verantwoordelijkheid volledig bij de dienstverlener zou moeten liggen.
- Online beschikbare security.txt: 13% geeft aan dat de volledige verantwoordelijkheid ligt bij de dienstverlener, terwijl 18% zegt dat de volledige verantwoordelijkheid bij de dienstverlener zou moeten liggen.

Er is één uitzondering hierop: het vergroten van bewustzijn onder medewerkers door training. De verantwoordelijkheid hiervoor moet volgens dienstverleners meer bij de afnemer komen te liggen; 17% van de dienstverleners zegt dat dit nu volledig bij de afnemer ligt, terwijl 22% vindt dat de verantwoordelijkheid volledig bij de afnemer zou moeten liggen.

Hoewel dit verschil minder sterk is dan bij dienstverleners, zou ook volgens afnemers de verantwoordelijkheid wat meer naar de dienstverlener moeten dan nu het geval is:

- Firewall: 15% van afnemers geeft aan dat dit nu volledig bij de dienstverlener ligt, terwijl 20% zegt dat het volledig bij de dienstverlener zou moeten liggen.
- Verplicht gebruik sterke wachtwoorden: 49% zegt dat de verantwoordelijkheid momenteel volledig bij de afnemer ligt, terwijl 44% zegt dat het volledig bij de afnemer zou moeten liggen
- Multifactor authenticatie: 5% zegt dat de verantwoordelijkheid volledig bij de dienstverlener ligt, terwijl 11% zegt dat de verantwoordelijkheid bij de dienstverlener zou moeten liggen
- Beveiligde internetverbindingen: 10% zegt dat het nu volledig de verantwoordelijkheid is van de dienstverlener, terwijl 17% zegt dat het de volledige verantwoordelijkheid van de dienstverlener zou moeten zijn.

motivaction
insights and strategy



Resultaten Cyberkennis:

Kennis & advies over cybersecurity

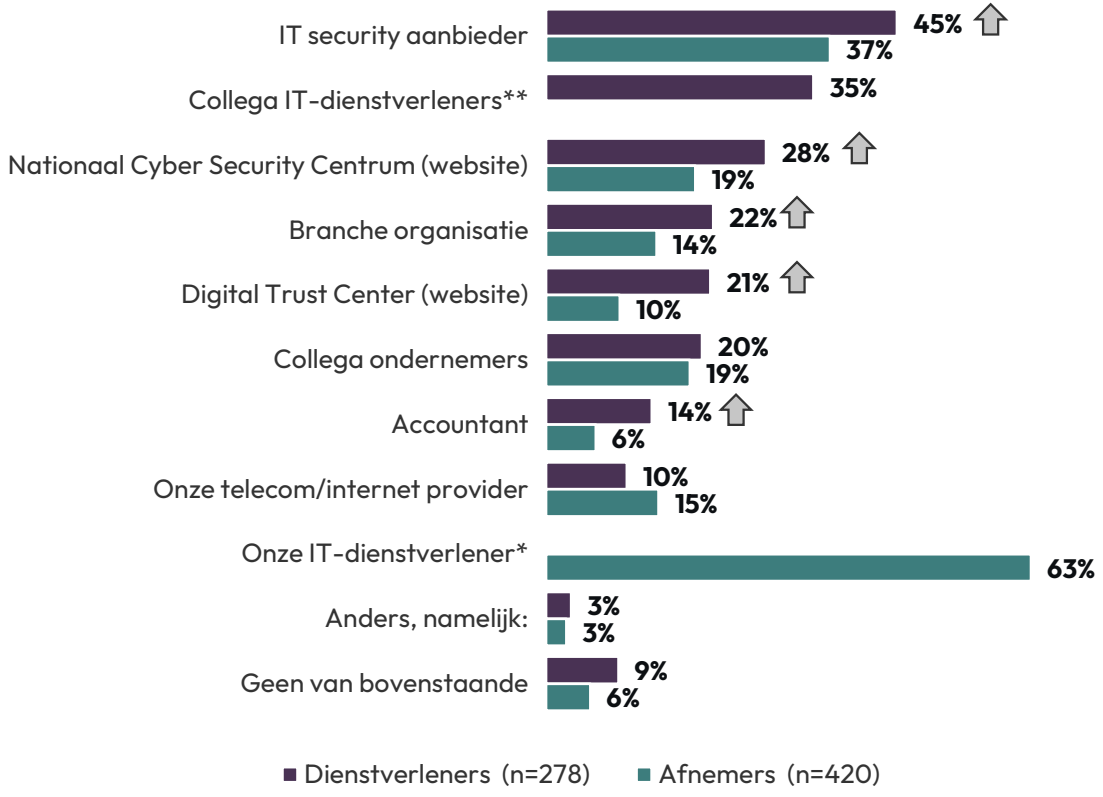
Afnemers gaan vooral naar hun dienstverlener voor advies; dienstverleners gaan vooral naar een IT security aanbieder of collega dienstverleners

Dienstverleners zeggen vaker dan afnemers advies te zoeken bij:

- IT security aanbieders (45% vs. 37%),
- het NCSC (28% vs. 19%),
- de branche organisatie (22% vs. 14%),
- het DTC (21% vs. 10%), en
- de accountant (14% vs. 6%)

Digitaal veilige afnemers zoeken vaker advies bij het NSCS (28% vs. 19%) en **digitaal waakzame afnemers** vaker bij collega ondernemers (26% vs. 19%).

Afnemers/Dienstverleners: Als je op zoek gaat naar advies over IT security/digitale veiligheid, waar of bij wie ga je dan op zoek naar informatie?
(Basis – allen)



Deze antwoordoptie is alleen voorgelegd aan afnemers
*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

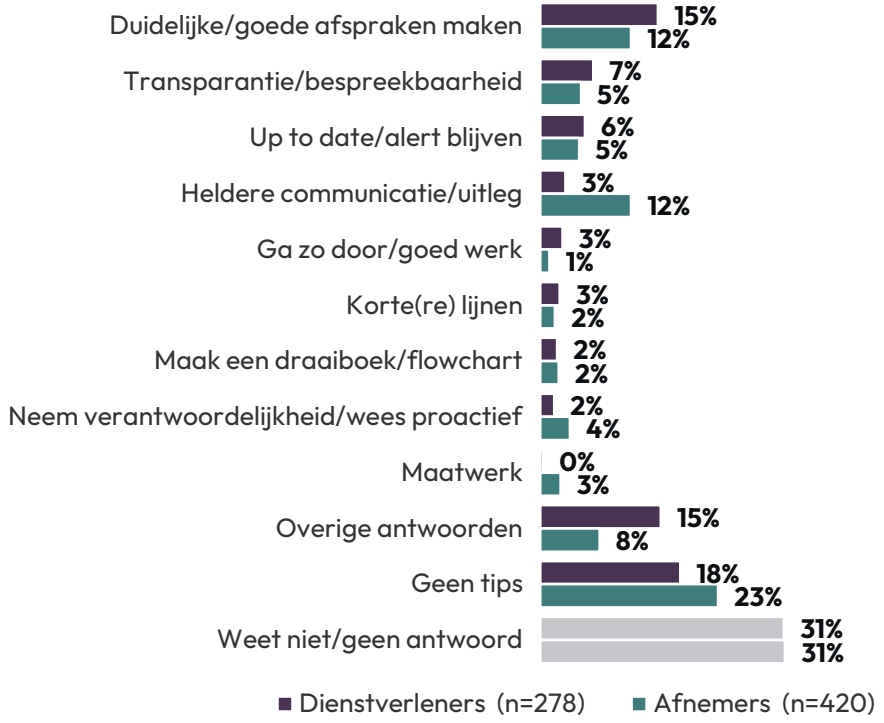
⇧ = vaker genoemd door dienstverleners dan door afnemers
⇩ = minder vaak genoemd door dienstverleners dan door afnemers

Klik hier voor de tabellen.

Dienstverleners en afnemers geven elkaar voornamelijk tips over goede afspraken en communicatie

Er zijn geen (grote, significante) verschillen tussen verschillende groepen.

Afnemers: Welke tip zou jij als IT-afnemer aan IT-dienstverleners willen meegeven om meer duidelijkheid te krijgen bij wie waarvoor verantwoordelijk m.b.t. cybersecurity?
Dienstverleners: Welke tip zou jij als IT-dienstverlener aan IT-afnemers willen meegeven om meer duidelijkheid te krijgen bij wie waarvoor verantwoordelijk m.b.t. cybersecurity?
(Basis – allen)



Respondenten konden hier zelf een antwoord typen. Deze antwoorden zijn later gecodeerd in een aantal categorieën.

Klik hier voor de tabellen.

Bijlagen: Onderzoekstechnische informatie

Bijlage - Onderzoekstechnische informatie

Veldwerkperiode
Het veldwerk is uitgevoerd in de periode 20-02-2025 tot 10-03-2025.

Methode respondentenselectie
Uit het StemPunt-panel van Motivaction.
Door een gespecialiseerd respondentenselectiebureau.

Incentives
De respondenten hebben als dank voor deelname aan het onderzoek punten voor het StemPunt spaarprogramma ontvangen.

Inschakelen externe leveranciers
Voor de volgende werkzaamheden heeft Motivaction bij dit onderzoek gebruik gemaakt van de diensten van gespecialiseerde bedrijven: respondentenselectie.

Responsverantwoording online onderzoek
In de veldwerkperiode is aan 11.548 personen een uitnodigingsmail gestuurd. Op de slotdatum van het veldwerk (zie bij Veldwerkperiode) was het gewenste aantal ingevulde vragenlijsten niet bereikt. In overleg met DTC is besloten de toegang tot de vragenlijst af te sluiten op de genoemde slotdatum.

Bewaartermijn primaire onderzoeksbestanden
Digitaal beschikbare primaire onderzoeksbestanden worden tot tenminste 12 maanden na afronden van het onderzoek bewaard. Hetzelfde geldt voor schriftelijke primaire bestanden zoals ingevulde vragenlijsten. Een uitzondering vormen beeld- en geluidsopnames van respondenten, deze worden ten hoogste 6 maanden bewaard.

Overige onderzoekstechnische informatie
Overige onderzoekstechnische informatie en een exemplaar van de bij dit onderzoek gehanteerde vragenlijst is op aanvraag beschikbaar voor de opdrachtgever.

Bijlage - Branches

Dienstverleners: In welke branche(s) werken de bedrijven aan wie jullie IT-diensten leveren?

Branche	Dienstverleners (n=278)
Financiële dienstverlening	29%
Informatie en communicatie	26%
Industrie	23%
Handel	21%
Energievoorziening	18%
Openbaar bestuur en overheidsdiensten	15%
Gezondheids- en welzijnszorg	14%
Vervoer en opslag	14%
Specialistische zakelijke diensten	13%
Waterbedrijven en afvalbeheer	11%
Bouwnijverheid	11%
Onderwijs	8%
Horeca	6%
Landbouw, bosbouw en visserij	4%
Verhuur en overige zakelijke diensten	4%
Cultuur, sport en recreatie	4%
Verhuur en handel van onroerend goed	3%
Delfstoffenwinning	3%
Overige dienstverlening (niet zakelijk)	3%
Anders, namelijk:	1%

Afnemers: Tot welke branche kan de organisatie waar je werkzaam bent gerekend worden?

Branche	Afnemers (n=420)
Financiële dienstverlening	15%
Gezondheids- en welzijnszorg	12%
Handel	12%
Specialistische zakelijke diensten	9%
Industrie	8%
Vervoer en opslag	5%
Onderwijs	5%
Cultuur, sport en recreatie	5%
Overige dienstverlening (niet zakelijk)	4%
Informatie en communicatie	4%
Horeca	3%
Bouwnijverheid	3%
Verhuur en handel van onroerend goed	3%
Verhuur en overige zakelijke diensten	2%
Landbouw, bosbouw en visserij	2%
Energievoorziening	2%
Delfstoffenwinning	0%
Waterbedrijven en afvalbeheer	0%
Anders, namelijk:	5%

Bijlage - Gehanteerde definities van IT-diensten/-producten

In dit onderzoek zijn de volgende definities gehanteerd van IT-diensten/-producten:

Cloud & Datacenter Services
Cloud & Datacenter Services levert cloud- en datacenterinfrastructuur, cross- en interconnectiediensten met andere datacenters en hyperscalers.
Producten en diensten die hieronder vallen zijn: Colocatie, inter-connectivity, data-architectuur, back-up, disaster recovery, cloud management en technisch applicatiebeheer.

Werkplek & End-user Services
Werkplek & End-user Services zijn services die direct voor eindgebruikers zichtbaar zijn.
Producten en diensten die hieronder vallen zijn: Werkplek Support, System integration, Service desk en On-site support.

Software Services
Software Services richt zich op de ontwikkeling van applicaties en/of digitale producten voor klanten.
Producten en diensten die hieronder vallen zijn: Maatwerk softwareontwikkeling, DevOps services, low-code/no-code en modern software engineering.

Security Services
Security Services zorgen ervoor dat een ICT-omgeving veilig is.
Producten en diensten die hieronder vallen zijn: SOC services, Vulnarability management, pen testing, Monitoring, Intelligence en Cloud security operations (SecOps).

Platform & Data Services
Platform Services zijn services om platform die partijen als SAP, ServiceNow, Salesforce, Microsoft en Oracle aanbieden succesvol te laten zijn binnen organisaties. Data services zijn services die ervoor zorgen dat organisaties informatie en kennis uit data kunnen krijgen.
Producten en diensten die hieronder vallen zijn: Platform management, Functioneel beheer platformen (ERP/CRM) en Data Intelligence.

Bijlagen: Toegankelijke tabellen

Ervaring met cyberincidenten

Doelgroep	Cyberincident	% Ja	% Nee	% Weet ik niet
Dienstverleners (n=278)	Ontvangen phishing mails van andere bedrijven	67%	22%	12%
Afnemers (n=420)	Ontvangen phishing mails van andere bedrijven	68%	27%	5%
Dienstverleners (n=278)	Verstuurde phishing mails uit naam van het bedrijf waar je werkt	55%	30%	14%
Afnemers (n=420)	Verstuurde phishing mails uit naam van het bedrijf waar je werkt	37%	52%	11%
Dienstverleners (n=278)	Datalek	49%	37%	14%
Afnemers (n=420)	Datalek	25%	64%	11%
Dienstverleners (n=278)	Onherkenbare foutieve inlogpogingen	47%	36%	17%
Afnemers (n=420)	Onherkenbare foutieve inlogpogingen	28%	57%	15%
Dienstverleners (n=278)	Mensen/bedrijven die gegevens opvragen en zich voordoen als een vermoedelijke klant, collega of leverancier	47%	38%	14%
Afnemers (n=420)	Mensen/bedrijven die gegevens opvragen en zich voordoen als een vermoedelijke klant, collega of leverancier	38%	50%	11%
Dienstverleners (n=278)	Dat door het downloaden van geïnfecteerde software/bestanden een virus werd verspreid	46%	38%	15%
Afnemers (n=420)	Dat door het downloaden van geïnfecteerde software/bestanden een virus werd verspreid	24%	66%	10%
Dienstverleners (n=278)	Insider threat	43%	39%	18%
Afnemers (n=420)	Insider threat	15%	72%	12%
Dienstverleners (n=278)	DDoS aanval waardoor de website van het bedrijf (tijdelijk) onbereikbaar was	43%	42%	15%
Afnemers (n=420)	DDoS aanval waardoor de website van het bedrijf (tijdelijk) onbereikbaar was	15%	76%	9%
Dienstverleners (n=278)	Ransomware	40%	46%	13%
Afnemers (n=420)	Ransomware	15%	78%	7%
Dienstverleners (n=278)	Identiteitsdiefstal	38%	48%	14%
Afnemers (n=420)	Identiteitsdiefstal	14%	75%	11%

Subjectieve mate van voorbereidheid op cyberincidenten

Mate van bereidheid	Dienstverleners (n=278)	Afnemers (n=420)
Volledig voorbereid	11%	7%
Goed voorbereid	37%	32%
Voorbereid	35%	30%
Matig voorbereid	14%	23%
Slecht voorbereid	2%	5%
Niet voorbereid	2%	2%

Concrete mate van voorbereidheid op cyberincidenten

Mate van voorbereidheid	Afnemers (n=420)	Dienstverleners (n=278)
We hebben het crisisplan geoefend en geëvalueerd (volledig voorbereid)	16%	15%
Er ligt een plan op hoofdlijnen; betrokkenen weten hoe zij moeten handelen (goed voorbereid)	26%	37%
Er zijn vaste afspraken in het geval van cyberincidenten waardoor netwerken, systemen en data meer dan 24 uur niet bereikbaar zijn (voorbereid)	15%	27%
Met de belangrijkste betrokkenen is alles op hoofdlijnen doorgesproken (matig voorbereid)	14%	7%
Het is wel eens besproken, maar het wordt ad hoc opgelost als het zich aandient (slecht voorbereid)	21%	8%
In het onderlinge contact tussen de organisaties is hier eigenlijk nog nooit over gesproken (niet voorbereid)	9%	5%

Reden om geen vaste afspraken/plannen te hebben ter voorbereiding op cyberincidenten

Redenen	Afnemers (n=282)	Dienstverleners (n=75)
Afnemers: We vertrouwen op onze IT-dienstverleners / Dienstverleners: Er is vertrouwen in de diensten van de IT-dienstverlener	39%	20%
Afnemers: De kans is klein dat dit het bedrijf waar ik werk overkomt / Dienstverleners: De kans is klein dat dit een van beide bedrijven overkomt	40%	18%
Afnemers: Investering is te hoog in verhouding tot de risico's / Dienstverleners: Investering is voor ons beiden te hoog in verhouding tot de risico's	17%	18%
Afnemers: We hebben er nog nooit goed over nagedacht / Dienstverleners: Er is nog nooit goed over nagedacht	22%	14%
Afnemers: We kunnen het toch niet voorkomen, hackers vinden altijd wel een manier / Dienstverleners: Het valt niet te voorkomen, hackers vinden altijd wel een manier	6%	12%
Afnemers: We hebben geen tijd om ons hiermee bezig te houden / Dienstverleners: Er is geen tijd om deze afspraken/plannen op te stellen	10%	12%
Afnemers: We weten niet hoe we dat moeten regelen / Dienstverleners: Het is niet duidelijk hoe we dat samen moeten regelen	8%	9%
We hebben geen zin om ons hierin te verdiepen*	7%	0%
Anders, namelijk:	3%	4%
Weet niet	3%	27%

**Deze antwoordoptie is alleen voorgelegd aan afnemers*

*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

Manier van samenwerking tussen dienstverleners en afnemers

Doelgroep	Manier	Zeer oneens	Oneens	Eens	Zeer eens	Weet niet/geen antwoord
Dienstverleners (n=278)	We hebben vaste contactpersonen die elkaar weten te vinden in het geval van cyberdreigingen/-aanvallen	2%	11%	49%	28%	10%
Afnemers (n=420)	We hebben vaste contactpersonen die elkaar weten te vinden in het geval van cyberdreigingen/-aanvallen	4%	13%	54%	20%	10%
Dienstverleners (n=278)	We werken volgens afspraken die hiervoor zijn opgenomen in het contract en de SLA als het bedrijf wordt getroffen door een cyberincident	1%	12%	50%	26%	12%
Afnemers (n=420)	We werken volgens afspraken die hiervoor zijn opgenomen in het contract en de SLA als het bedrijf wordt getroffen door een cyberincident	8%	12%	49%	14%	18%
Dienstverleners (n=278)	We hebben gezamenlijk de risico's voor cyberdreigingen/-aanvallen voor het bedrijf vastgesteld	3%	12%	47%	27%	13%
Afnemers (n=420)	We hebben gezamenlijk de risico's voor cyberdreigingen/-aanvallen voor het bedrijf vastgesteld	7%	19%	48%	11%	16%
Dienstverleners (n=278)	We hebben een gezamenlijk draaiboek klaarliggen voor als het bedrijf wordt getroffen door een cyberincident	2%	13%	47%	25%	13%
Afnemers (n=420)	We hebben een gezamenlijk draaiboek klaarliggen voor als het bedrijf wordt getroffen door een cyberincident	9%	23%	42%	11%	15%
Dienstverleners (n=278)	We testen/oefenen regelmatig het gezamenlijk draaiboek voor als het bedrijf wordt getroffen door een cyberincident	5%	14%	48%	21%	12%
Afnemers (n=420)	We testen/oefenen regelmatig het gezamenlijk draaiboek voor als het bedrijf wordt getroffen door een cyberincident	14%	27%	34%	9%	17%
Dienstverleners (n=278)	We werken op basis van vertrouwen dat komt vast ook goed als het bedrijf wordt getroffen door een cyberincident	3%	19%	43%	19%	15%
Afnemers (n=420)	We werken op basis van vertrouwen dat komt vast ook goed als het bedrijf wordt getroffen door een cyberincident	7%	18%	48%	11%	15%

Mate van zorgen om cybersecurity

Mate van zorgen	Dienstverleners (n=278)	Afnemers (n=420)
1 t/m 5 (geen/weinig zorgen)	21%	40%
6	12%	19%
7	21%	21%
8	27%	16%
9	13%	2%
10 (zeer veel zorgen)	5%	2%
Gemiddelde	6,8	5,7

Reden voor weinig zorgen

Reden	Afnemers (n=169)	Dienstverleners (n=59)
Afnemers: We vertrouwen op onze Telecom en IT-dienstverleners / Dienstverleners: We hebben vertrouwen in de maatregelen die wij als IT-dienstverlener genomen hebben	43%	64%
Afnemers: We hebben genoeg maatregelen getroffen om een cyberincident te voorkomen / Dienstverleners: We vertrouwen erop dat onze IT-afnemers genoeg maatregelen getroffen hebben om een cyberincident te voorkomen	46%	36%
Afnemers: De kans is klein dat dit het bedrijf waar ik werk overkomt / Dienstverleners: Wij achten de kans klein dat dit hun bedrijf overkomt	39%	19%
Ze hebben een andere IT-dienstverlener die hen helpt bij (ernstige) cyberincidenten**	0%	17%
We kunnen het toch niet voorkomen, hackers vinden altijd wel een manier*	16%	0%
Als een cyberincident zich voordoet, zal dit toch geen/weinig impact hebben*	22%	0%
Anders, namelijk:	3%	3%
Weet niet	4%	12%

**Deze antwoordoptie is alleen voorgelegd aan afnemers*

*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

Reden voor zorgen

Reden	Afnemers (n=251)	Dienstverleners (n=219)
De impact van een cyberincident is groot	48%	42%
Onze IT-afnemers hebben ook andere IT-dienstverleners die zich niet goed hebben voorbereid op een cyberincident**	0%	30%
Onze IT-dienstverlener(s)/Onze IT-afnemer(s) houd(en) zich niet altijd aan de afspraken die we samen hebben gemaakt	10%	27%
Wij/Onze IT-afnemers hebben niet genoeg maatregelen getroffen om een cyberincident te voorkomen	20%	26%
Wij zien het niet als onze verantwoordelijkheid	10%	22%
Wij achten de kans groot dat dit het bedrijf overkomt	21%	21%
Anders, namelijk:	5%	1%
Weet niet	13%	5%

**Deze antwoordoptie is alleen voorgelegd aan afnemers*

*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

Digitale bekwaamheid en bewustheid

Mate van bekwaamheid en bewustheid	Afnemers (n=420)	Dienstverleners (n=278)
Digitaal veilig (bewust - bekwaam)	23%	30%
Digitaal waakzaam (bewust - onbekwaam)	29%	29%
Digitaal overmoedig (onbewust - bekwaam)	12%	15%
Praktisch digitaal (onbewust - onbekwaam)	35%	26%

Verantwoordelijkheid voor digitale veiligheid (Security Services)

Verantwoordelijkheid	Afnemers (n=171)	Dienstverleners (n=120)
De IT-afnemer is volledig verantwoordelijk	23%	7%
De IT-afnemer is meer verantwoordelijk dan de IT-dienstverlener(s) van Security Services	23%	31%
De IT-afnemer en de IT-dienstverlener(s) van Security Services hebben gedeelde verantwoordelijkheid	42%	41%
De IT-dienstverlener(s) van Security Services zijn meer verantwoordelijk dan de IT-afnemer	11%	18%
De IT-dienstverlener(s) van Security Services zijn volledig verantwoordelijk	1%	3%

Verantwoordelijkheid voor digitale veiligheid (algemeen)

Verantwoordelijkheid	Afnemers (n=420)	Dienstverleners (n=278)
De IT-afnemer is volledig verantwoordelijk	24%	12%
De IT-afnemer is meer verantwoordelijk dan de IT-dienstverlener(s)	22%	26%
De IT-afnemer en de IT-dienstverlener(s) hebben gedeelde verantwoordelijkheid	43%	44%
De IT-dienstverlener(s) zijn meer verantwoordelijk dan de IT-afnemer	9%	13%
De IT-dienstverlener(s) zijn volledig verantwoordelijk	2%	6%

Verantwoordelijkheid van dienstverleners van Cloud & Datacenter Services

Antwoorden	Afnemers (n=184)	Dienstverleners (n=102)
Adequate beveiliging (algemeen)	10%	17%
De volledige verantwoordelijkheid (algemeen)	10%	11%
Gedeelde verantwoordelijkheid	8%	8%
Monitoren van eventuele problemen	2%	6%
Een goed beveiligde cloud	11%	5%
Een goed beveiligd datacenter	5%	4%
Het faciliteren van een goed beveiligde toegang/inlog	3%	3%
Het opslaan van data (algemeen)	3%	3%
De klant goed informeren aangaande risico's/nodige maatregelen	3%	3%
Up-to-date blijven/software updates blijven uitvoeren	5%	3%
Operationaliteit (algemeen)	1%	3%
Een goede backup	5%	1%
Tijdige signalering van problemen	1%	1%
Goede herstelprocedures	2%	0%
Overige antwoorden	15%	19%
Weet niet/geen antwoord	33%	32%

Verantwoordelijkheid van dienstverleners van Werkplek & End-user Services

Antwoorden	Afnemers (n=173)	Dienstverleners (n=100)
Afscherming/beveiliging netwerken	2%	10%
(Tijdig) faciliteren van trainingen/bewustzijn	5%	8%
De beveiliging (algemeen)	9%	7%
Up-to-date blijven/software updates blijven uitvoeren	8%	7%
De volledige verantwoordelijkheid (algemeen)	5%	6%
Het faciliteren van een goed beveiligde toegang/inlog	3%	5%
Ondersteuning bieden/bereikbaar zijn (algemeen)	3%	5%
Afhankelijk van het contract/afspraken nakomen	6%	3%
Beveiliging/bescherming van gegevens/privacy/data	1%	2%
De klant goed informeren aangaande risico's/nodige maatregelen	2%	1%
Monitoren van eventuele problemen	5%	0%
Overige antwoorden	21%	18%
Weet niet/geen antwoord	38%	40%

Verantwoordelijkheid van dienstverleners van Software Services

Antwoorden	Afnemers (n=189)	Dienstverleners (n=111)
Levering van beveiligde/betrouwbare software	5%	15%
Up-to-date blijven/software updates blijven uitvoeren	12%	7%
De klant goed informeren aangaande risico's/nodige maatregelen	4%	6%
Monitoren/signaleren van eventuele problemen	7%	5%
De volledige verantwoordelijkheid (algemeen)	3%	3%
Het bedrijf is na software afname ook zelf verantwoordelijk	3%	3%
Gedeelde verantwoordelijkheid (algemeen)	8%	2%
Afhankelijk van het contract/afspraken nakomen	4%	1%
Overige antwoorden	28%	41%
Weet niet/geen antwoord	34%	31%

Verantwoordelijkheid van dienstverleners van Security Services

Antwoorden	Afnemers (n=148)	Dienstverleners (n=107)
Goede beveiliging (algemeen)	9%	14%
De volledige verantwoordelijkheid (algemeen)	6%	12%
Monitoren/signaleren van eventuele problemen	11%	12%
De klant goed informeren aangaande risico's/nodige maatregelen	11%	8%
Up-to-date blijven/software updates blijven uitvoeren	9%	8%
Gedeelde verantwoordelijkheid (algemeen)	5%	7%
Afhankelijk van het contract/afspraken nakomen	6%	7%
Wil ik niet zeggen (omwille van privacy)	2%	3%
Het bedrijf is na software afname ook zelf verantwoordelijk	1%	1%
Operationaliteit (algemeen)	3%	0%
Grote/meeste verantwoordelijkheid	5%	0%
Overige antwoorden	12%	17%
Weet niet/geen antwoord	33%	28%

Verantwoordelijkheid van dienstverleners van Platform & Data Services

Antwoorden	Afnemers (n=159)	Dienstverleners (n=105)
De volledige verantwoordelijkheid (algemeen)	6%	12%
Beveiliging/bescherming van gegevens/privacy/data	5%	12%
Goede beveiliging (algemeen)	14%	10%
Gedeelde verantwoordelijkheid (algemeen)	9%	7%
Monitoren/signaleren van eventuele problemen	9%	5%
Afhankelijk van het contract/afspraken nakomen	7%	4%
Up-to-date blijven/software updates blijven uitvoeren	10%	2%
Operationaliteit (algemeen)	1%	1%
Een goede backup	1%	0%
De klant goed informeren aangaande risico's/nodige maatregelen	1%	0%
Overige antwoorden	14%	15%
Weet niet/geen antwoord	37%	41%

Verantwoordelijkheid voor uitvoer (1/3)

Doelgroep	Manier	Uitvoer ligt volledig bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-dienstverlener	Uitvoer ligt volledig bij de IT-dienstverlener	Weet ik niet
Dienstverleners (n=278)	**Bedrijfsbreed uitrollen beveiligingsupdates indien beschikbaar ('patchen')**	2%	11%	49%	28%	10%
Afnemers (n=420)	**Bedrijfsbreed uitrollen beveiligingsupdates indien beschikbaar ('patchen')**	4%	13%	54%	20%	10%
Dienstverleners (n=278)	**Actieve monitoring en detectie**	10%	24%	38%	15%	12%
Afnemers (n=420)	**Actieve monitoring en detectie**	21%	20%	29%	14%	17%
Dienstverleners (n=278)	**Netwerk segmentatie om dreiging in het gehele netwerk te voorkomen**	13%	25%	36%	17%	9%
Afnemers (n=420)	**Netwerk segmentatie om dreiging in het gehele netwerk te voorkomen**	22%	20%	25%	12%	19%
Dienstverleners (n=278)	**Firewall voor alle systemen verbonden met internet**	13%	26%	33%	19%	9%
Afnemers (n=420)	**Firewall voor alle systemen verbonden met internet**	28%	18%	28%	15%	11%
Dienstverleners (n=278)	**Functionaliteit beperken of uitschakelen waar deze onnodig is of een te groot risico vormt (‘hardening’)**	13%	24%	41%	10%	12%
Afnemers (n=420)	**Functionaliteit beperken of uitschakelen waar deze onnodig is of een te groot risico vormt (‘hardening’)**	25%	26%	23%	7%	18%
Dienstverleners (n=278)	**Automatische back-up van systemen**	12%	28%	32%	19%	8%
Afnemers (n=420)	**Automatische back-up van systemen**	28%	24%	22%	18%	9%

Verantwoordelijkheid voor uitvoer (2/3)

Doelgroep	Manier	Uitvoer ligt volledig bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-dienstverlener	Uitvoer ligt volledig bij de IT-dienstverlener	Weet ik niet
Dienstverleners (n=278)	**Encryptie/versleuteling van belangrijke data**	11%	29%	33%	18%	9%
Afnemers (n=420)	**Encryptie/versleuteling van belangrijke data**	24%	22%	25%	12%	18%
Dienstverleners (n=278)	**Beveiligde internetverbindingen (bijvoorbeeld standaard afgedwongen HTTPS)**	12%	29%	33%	18%	8%
Afnemers (n=420)	**Beveiligde internetverbindingen (bijvoorbeeld standaard afgedwongen HTTPS)**	27%	22%	25%	10%	15%
Dienstverleners (n=278)	**Draaiboek opgesteld hoe te handelen bij een cyberincident**	11%	28%	37%	14%	11%
Afnemers (n=420)	**Draaiboek opgesteld hoe te handelen bij een cyberincident**	27%	28%	20%	5%	20%
Dienstverleners (n=278)	**Er is een risico-analyse uitgevoerd waarna passende maatregelen zijn getroffen**	12%	28%	36%	14%	11%
Afnemers (n=420)	**Er is een risico-analyse uitgevoerd waarna passende maatregelen zijn getroffen**	23%	26%	22%	7%	22%
Dienstverleners (n=278)	**Antivirus software**	17%	27%	29%	18%	8%
Afnemers (n=420)	**Antivirus software**	32%	18%	25%	15%	10%
Dienstverleners (n=278)	**Rechten voor toegang tot gevoelige data worden weloverwogen toegekend**	14%	32%	32%	13%	10%
Afnemers (n=420)	**Rechten voor toegang tot gevoelige data worden weloverwogen toegekend**	41%	27%	14%	5%	13%

Verantwoordelijkheid voor uitvoer (3/3)

Doelgroep	Manier	Uitvoer ligt volledig bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-afnemers	Uitvoer ligt voornamelijk bij de IT-dienstverlener	Uitvoer ligt volledig bij de IT-dienstverlener	Weet ik niet
Dienstverleners (n=278)	**Ingeschreven op bronnen over kwetsbaarheden en veiligheid**	12%	31%	31%	12%	14%
Afnemers (n=420)	**Ingeschreven op bronnen over kwetsbaarheden en veiligheid**	23%	21%	23%	7%	26%
Dienstverleners (n=278)	**Verplicht gebruik sterke wachtwoorden**	19%	29%	28%	14%	9%
Afnemers (n=420)	**Verplicht gebruik sterke wachtwoorden**	49%	19%	15%	6%	10%
Dienstverleners (n=278)	**Multifactor authenticatie voor toegang tot belangrijkste systemen**	15%	34%	28%	14%	9%
Afnemers (n=420)	**Multifactor authenticatie voor toegang tot belangrijkste systemen**	39%	25%	20%	5%	11%
Dienstverleners (n=278)	**Security.txt of hoe we omgaan met responsible disclosure-meldingen is online vindbaar**	12%	29%	29%	13%	18%
Afnemers (n=420)	**Security.txt of hoe we omgaan met responsible disclosure-meldingen is online vindbaar**	21%	16%	19%	7%	37%
Dienstverleners (n=278)	**Rechten voor toegang tot gevoelige data zijn altijd up-to-date**	17%	34%	26%	14%	9%
Afnemers (n=420)	**Rechten voor toegang tot gevoelige data zijn altijd up-to-date**	38%	25%	17%	7%	14%
Dienstverleners (n=278)	**Vergroting bewustzijn medewerkers (door training)**	17%	37%	27%	10%	9%
Afnemers (n=420)	**Vergroting bewustzijn medewerkers (door training)**	48%	25%	13%	3%	12%
Dienstverleners (n=278)	**Cyberverzekering afgesloten**	27%	25%	21%	9%	18%
Afnemers (n=420)	**Cyberverzekering afgesloten**	33%	16%	15%	5%	31%

Gewenste verantwoordelijkheid voor uitvoer (1/3)

Doelgroep	Manier	Uitvoer zou volledig bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-dienstverlener moeten liggen	Uitvoer zou volledig bij de IT-dienstverlener moeten liggen	Weet ik niet
Dienstverleners (n=278)	**Netwerk segmentatie om dreiging in het gehele netwerk te voorkomen**	13%	21%	39%	19%	8%
Afnemers (n=420)	**Netwerk segmentatie om dreiging in het gehele netwerk te voorkomen**	22%	18%	28%	15%	17%
Dienstverleners (n=278)	**Actieve monitoring en detectie**	12%	23%	36%	22%	8%
Afnemers (n=420)	**Actieve monitoring en detectie**	21%	19%	28%	19%	14%
Dienstverleners (n=278)	**Automatische back-up van systemen**	13%	24%	33%	23%	6%
Afnemers (n=420)	**Automatische back-up van systemen**	26%	20%	23%	18%	12%
Dienstverleners (n=278)	**Bedrijfsbreed uitrollen beveiligingsupdates indien beschikbaar ('patchen')**	13%	24%	33%	22%	9%
Afnemers (n=420)	**Bedrijfsbreed uitrollen beveiligingsupdates indien beschikbaar ('patchen')**	25%	21%	21%	17%	15%
Dienstverleners (n=278)	**Antivirus software**	14%	22%	33%	21%	9%
Afnemers (n=420)	**Antivirus software**	30%	21%	22%	17%	10%
Dienstverleners (n=278)	**Beveiligde internetverbindingen (bijvoorbeeld standaard afgedwongen HTTPS)**	11%	26%	32%	21%	10%
Afnemers (n=420)	**Beveiligde internetverbindingen (bijvoorbeeld standaard afgedwongen HTTPS)**	26%	19%	24%	17%	15%
Dienstverleners (n=278)	**Er is een risico-analyse uitgevoerd waarna passende maatregelen zijn getroffen**	12%	27%	37%	16%	8%
Afnemers (n=420)	**Er is een risico-analyse uitgevoerd waarna passende maatregelen zijn getroffen**	28%	24%	24%	11%	14%

Gewenste verantwoordelijkheid voor uitvoer (2/3)

Doelgroep	Manier	Uitvoer zou volledig bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-dienstverlener moeten liggen	Uitvoer zou volledig bij de IT-dienstverlener moeten liggen	Weet ik niet
Dienstverleners (n=278)	**Firewall voor alle systemen verbonden met internet**	14%	23%	31%	22%	10%
Afnemers (n=420)	**Firewall voor alle systemen verbonden met internet**	25%	19%	24%	20%	12%
Dienstverleners (n=278)	**Encryptie/versleuteling van belangrijke data**	13%	26%	29%	24%	8%
Afnemers (n=420)	**Encryptie/versleuteling van belangrijke data**	25%	22%	23%	16%	14%
Dienstverleners (n=278)	**Ingeschreven op bronnen over kwetsbaarheden en veiligheid**	12%	27%	34%	15%	12%
Afnemers (n=420)	**Ingeschreven op bronnen over kwetsbaarheden en veiligheid**	24%	20%	22%	11%	22%
Dienstverleners (n=278)	**Security.txt of hoe we omgaan met responsible disclosure-meldingen is online vindbaar**	12%	25%	32%	18%	14%
Afnemers (n=420)	**Security.txt of hoe we omgaan met responsible disclosure-meldingen is online vindbaar**	21%	20%	22%	11%	26%
Dienstverleners (n=278)	**Multifactor authenticatie voor toegang tot belangrijkste systemen**	18%	25%	29%	19%	9%
Afnemers (n=420)	**Multifactor authenticatie voor toegang tot belangrijkste systemen**	36%	24%	17%	11%	12%
Dienstverleners (n=278)	**Draaiboek opgesteld hoe te handelen bij een cyberincident**	13%	29%	33%	16%	9%
Afnemers (n=420)	**Draaiboek opgesteld hoe te handelen bij een cyberincident**	29%	29%	19%	8%	15%

Gewenste verantwoordelijkheid voor uitvoer (3/3)

Doelgroep	Manier	Uitvoer zou volledig bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-afnemers moeten liggen	Uitvoer zou voornamelijk bij de IT-dienstverlener moeten liggen	Uitvoer zou volledig bij de IT-dienstverlener moeten liggen	Weet ik niet
Dienstverleners (n=278)	**Functionaliteit beperken of uitschakelen waar deze onnodig is of een te groot risico vormt ('hardening')**	14%	27%	32%	16%	10%
Afnemers (n=420)	**Functionaliteit beperken of uitschakelen waar deze onnodig is of een te groot risico vormt ('hardening')**	25%	22%	27%	10%	16%
Dienstverleners (n=278)	**Rechten voor toegang tot gevoelige data worden weloverwogen toegekend**	16%	30%	33%	14%	8%
Afnemers (n=420)	**Rechten voor toegang tot gevoelige data worden weloverwogen toegekend**	40%	23%	18%	7%	13%
Dienstverleners (n=278)	**Rechten voor toegang tot gevoelige data zijn altijd up-to-date**	19%	27%	29%	17%	8%
Afnemers (n=420)	**Rechten voor toegang tot gevoelige data zijn altijd up-to-date**	38%	24%	15%	9%	13%
Dienstverleners (n=278)	**Verplicht gebruik sterke wachtwoorden**	20%	28%	26%	19%	7%
Afnemers (n=420)	**Verplicht gebruik sterke wachtwoorden**	44%	22%	16%	7%	10%
Dienstverleners (n=278)	**Vergroting bewustzijn medewerkers (door training)**	22%	29%	30%	11%	8%
Afnemers (n=420)	**Vergroting bewustzijn medewerkers (door training)**	47%	24%	14%	5%	11%
Dienstverleners (n=278)	**Cyberverzekering afgesloten**	24%	25%	26%	12%	13%
Afnemers (n=420)	**Cyberverzekering afgesloten**	36%	19%	13%	9%	23%

Informatiebron voor advies over cybersecurity

Informatiebron	Afnemers (n=420)	Dienstverleners (n=278)
IT security aanbieder	37%	45%
Collega IT-dienstverleners**	0%	35%
Nationaal Cyber Security Centrum (website)	19%	28%
Branche organisatie	14%	22%
Digital Trust Center (website)	10%	21%
Collega ondernemers	19%	20%
Accountant	6%	14%
Onze telecom/internet provider	15%	10%
Onze IT-dienstverlener*	63%	0%
Anders, namelijk:	3%	3%
Geen van bovenstaande	6%	9%

**Deze antwoordoptie is alleen voorgelegd aan afnemers*
*** Deze antwoordoptie is alleen voorgelegd aan dienstverleners*

Tips om meer duidelijkheid te krijgen over verantwoordelijkheid

Tip	Afnemers (n=420)	Dienstverleners (n=278)
Duidelijke/goede afspraken maken	12%	15%
Transparantie/bespreekbaarheid	5%	7%
Up to date/alert blijven	5%	6%
Heldere communicatie/uitleg	12%	3%
Ga zo door/goed werk	1%	3%
Korte(re) lijnen	2%	3%
Maak een draaiboek/flowchart	2%	2%
Neem verantwoordelijkheid/wees proactief	4%	2%
Maatwerk	3%	0%
Overige antwoorden	8%	15%
Geen tips	23%	18%
Weet niet/geen antwoord	31%	31%

Wij verminderen onze footprint

Motivaction gebruikt uitsluitend papier met een FSC-label

Motivaction gebruikt energiezuinige auto’s

Motivaction gebruikt groene stroom

Auteursrecht

meer zien
meer weten
meer betekenen

motivaction
insights and strategy

Motivaction International bv
Marnixkade 109F
1015ZL Amsterdam

Postbus 15262
1001MG Amsterdam

020 589 83 83

info@motivaction.nl
www.motivaction.nl