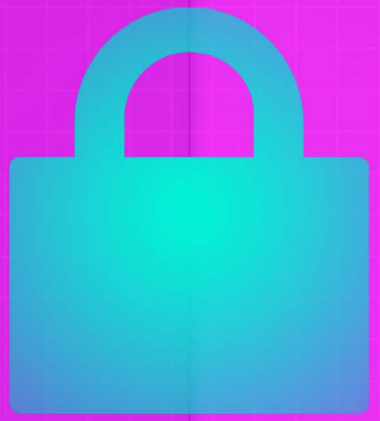
e-book

datto
A Kaseya COMPANY



Datto-rapport over cyberbeveiliging voor MSP's in het MKB

Een wereld van kansen voor MSP's

Kleine en middelgrote bedrijven (het MKB) worden geconfronteerd met toenemende uitdagingen op het gebied van cyberbeveiliging, waardoor veel MKB's hun inzet voor beveiliging en hun budgetten voor beveiliging hebben verhoogd. Er is ruimte voor MSP's om op vele gebieden omzetgroei te realiseren, waaronder beveiligd identiteits- en toegangsbeheer, endpoint-beveiliging, Business Continuity and Disaster Recovery (BCDR) en bescherming tegen phishing. De huidige wereld van toenemende cyberbedreigingen voor het MKB is een wereld van toenemende zakelijke kansen op het gebied van beveiliging voor MSP's over de hele wereld.

Wij hebben met 2.913 besluitvormers uit de IT-sector gesproken over hun beveiligingsproblemen, en wij delen die gegevens met u om u te helpen om uw MSP te laten groeien.

7 Belangrijkste punten

IT-professionals maken zich zorgen over beveiliging en zijn bereid om investeringen te doen om hun organisaties veilig te houden.

Het MKB ondervindt nog steeds aanzienlijke beveiligingsproblemen en erkent dat het geld moet uitgeven om deze op te lossen: ongeveer de helft van de respondenten in onze enquête is van plan geld uit te geven aan e-mailbeveiliging, back-ups en antivirusbescherming.

Veel MKB's hebben hulp nodig om zich voor te bereiden op het herstel na beveiligingsincidenten.

Meer dan de helft van onze respondenten van de enquête gaf toe dat een succesvolle phishing-aanval of, erger nog, een ransomware-aanval, hun organisatie ernstige schade zou toebrengen.

Weinig MKB's bezuinigen op beveiligingsuitgaven, maar investeren in beveiliging.

Vier op de tien respondenten van de enquête gaven aan dat hun organisatie de uitgaven voor cyberbeveiliging verhoogt, en de meesten verwachten dat dit zo zal blijven – uitstekend nieuws voor MSP's in de huidige uitdagende economie.

Phishing is het grootste beveiligingsprobleem voor het MKB.

IT-managers van bedrijven maken zich zorgen over phishing en het gevaar dat dit met zich meebrengt. Dit creëert mogelijkheden voor groei in inkomsten voor MSP's op het gebied van e-mailbeveiliging en beveiligingstraining met simulaties van phishing.

Downtime is kostbaar, maar veel bedrijven beschikken niet over de juiste hulpmiddelen om dit tot een minimum te beperken.

MSP's hebben een gouden kans om hun inkomsten uit te breiden en hun klanten te helpen om dure downtime te verminderen met oplossingen als BCDR, managed SOC en incident response planning.

MKB's vertrouwen vaak op uitbestede IT-beveiliging.

Bedrijven hebben hulp van buitenaf nodig om hun beveiliging te onderhouden en te verbeteren, en bijna de helft van de IT-professionals die wij hebben ondervraagd, zei dat hun organisatie vertrouwt op een MSP of MSSP om de klus te klaren.

Een groot aantal MKB's is niet gelukkig met hun huidige defensieve opbouw.

Een derde van onze respondenten zei ontevreden te zijn met hun huidige aanbod van oplossingen voor beveiliging, wat aangeeft dat er ruimte is voor MKB's om een plekje in de markt te veroveren.

Kaders voor cyberbeveiliging

NIST is niet het meest populaire kader

Zero-trust wordt sterk aanbevolen door deskundigen, maar slechts 14% van de respondenten zei dat hun organisatie dat kader gebruikt en slechts 7% was er bezorgd over, waardoor er veel ruimte is voor groei (en kansen voor MSP's) in dit gebied.

Kader of verordening	Niveau van gebruik	Niveau van bezorgdheid
CIS	34%	26%
CMMC	30%	26%
COBIT	27%	23%
NIST	22%	19%
ISO 27001	21%	15%
NCSC (National Cyber Security Center)	18%	20%
HIPAA	18%	13%
Zero Trust	14%	7%
ASD Essential 8	14%	13%
PCI-DSS	12%	10%
SOC II	11%	7%
MITRE ATT&CK	9%	9%
Overige	5%	N.v.t.
Geen	3%	27%

CIS en CMMC zijn de meest gebruikte en de meest relevante kaders voor cyberbeveiliging.

MKB's zijn proactief bij het beoordelen van kwetsbaarheden

De meerderheid van het MKB in alle regio's is geïnteresseerd in het in de gaten houden van hun kwetsbaarheden op het gebied van IT-beveiliging in een dergelijk onstabiel klimaat van cybercriminaliteit. Daarom zijn zij vooral geïnteresseerd in gebruiksvriendelijke oplossingen die het proces van beoordeling van de kwetsbaarheid snel en eenvoudig maken.

Frequentie van beoordelingen	Reacties
Meer dan 4x per jaar	13%
3 tot 4x per jaar	24%
Tweemaal per jaar	25%
Eenmaal per jaar	21%
Eens in de 2 tot 4 jaar	12%
Eens per 5 jaar of langer	3%
Nooit	1%
Weet ik niet	2%

Meer dan een derde van de respondenten voert drie of meer keer per jaar een evaluatie van de kwetsbaarheid van hun IT-beveiliging uit.

MKB's bezuinigen niet op beveiliging; de budgetten stijgen juist

In het licht van de stijgende cybercriminaliteit en een groeiend bewustzijn van de schade die een cyberaanval kan aanrichten bij niet-tech besluitvormers, zijn de beveiligingsbudgetten voor IT het afgelopen jaar gestegen. MKB's zijn optimistisch dat ze in 2023 stabiel blijven of stijgen. Dit biedt MSP's de mogelijkheid om klanten aan te moedigen tot uitgebreide verbeteringen en upgrades van de beveiliging.

IT-budgetten	Reacties
Verhoogd	42%
Gelijk gebleven	40%
Verlaagd	6%

Vier op de tien (42%) van de respondenten van de enquête melden dat ze hun beveiligingsbudget voor IT dit jaar hebben verhoogd.

Beveiliging is een flinke hap uit de meeste IT-budgetten

MKB-bedrijven hebben geld om te besteden aan beveiliging

% van het totale IT-budget	Reacties
Minder dan 1%	1%
1% –5%	10%
6% –10%	19%
11%–15%	19%
16%–20%	20%
21%–30%	15%
31%–40%	8%
41% –50%	5%
Meer dan 50%	3%

Bijna een derde van het MKB besteedt 20% tot 50% van zijn IT-budget aan beveiliging.

MKB's zijn op zoek naar hulp bij IT-beveiliging

Hoewel veel MKB's de beveiliging intern beheren, zijn er genoeg bedrijven die voor hun behoeften op het gebied van IT-beveiliging een beroep doen op MSP's en MSSP's. Het tekort aan technisch talent is een belangrijke factor, maar het gebrek aan expertise is ook een belangrijke motivator voor bedrijven om hun technisch werk uit te besteden. MSP's kunnen er baat bij hebben zich te positioneren als vakkundige, up-to-date deskundigen voor klanten en potentiële klanten.

Een op de vier besteedt zijn beveiliging uit aan een MSP, en een op de zes aan een MSSP.

Wie beheert uw IT-beveiliging?	Reacties
Gedeeltelijke interne IT	47%
Toegewijde interne IT	50%
Individuele outsourcing van IT	28%
Het bedrijf besteedt IT uit aan een IT-service provider of MSP	26%
Het bedrijf besteedt IT uit aan een MSSP	16%
Het bedrijf besteedt IT uit, maar weet niet zeker aan welk type dienstverlener	5%

Er is ruimte voor MSP's om een plekje in de markt te veroveren

Slechts 31% van de respondenten zegt volledig tevreden te zijn over hun beveiligingsoplossingen, waardoor MSP's kansen krijgen om te groeien.

Tevredenheidsniveau	Reacties
Volledig tevreden	31%
Enigszins tevreden	54%
Neutraal	12%
Enigszins ontevreden	2%
Volledig ontevreden	1%

Alleen 54%

van de bedrijven is enigszins tevreden over hun beveiligingsoplossingen.

De meeste bedrijven hebben de boodschap begrepen dat een herstelplan essentieel is voor het bedrijf.

Meer dan de helft van de respondenten zegt een standaard herstelplan klaar te hebben liggen. Sommige bedrijven hebben echter nog steeds serieuze hulp nodig bij het maken van een herstelplan, waardoor er voor MSP's kansen zijn om hen te helpen voorbereid te zijn op problemen. Het is ook een uitgelezen kans voor MSP's om klanten te begeleiden bij het investeren in de middelen die zij nodig hebben om dat plan uit te voeren, zoals BCDR of tools voor identiteits- en toegangsbeheer op afstand.

Acht op de tien respondenten (81%) zeggen dat hun bedrijf over een herstelplan beschikt.

Status herstelplan	Reacties
We hebben een best-in-class herstelplan	29%
We hebben een standaard herstelplan	52%
We hebben oplossingen om ons te beschermen, maar hebben geen formeel herstelplan	14%
We hebben geen herstelplan	2%
Ik geloof dat mijn service provider een herstelplan heeft, maar ik ken de details niet	3%

Beveiligingsproducten

Een sterke verdediging tegen ransomware voert de prioriteitenlijst van het MKB aan

In het tijdperk van ransomware is het geen verrassing dat antivirussoftware (57%) en e-mailbeveiliging (53%) bovenaan het lijstje van bedrijven staan.

De beveiligingsoplossingen die organisaties in de komende 12 maanden willen implementeren

Oplossing	Respondenten
Antivirussoftware	57%
Bescherming van e-mail/spam	53%
Back-up van bestanden	49%
Beheerde firewall	49%
Training op het gebied van cyberbeveiliging voor werknemers	43%
Identiteits- en toegangsbeheer	38%
Centrum voor beveiligingsactiviteiten	28%
Managed Detection and Response	27%
Business Continuity and Disaster Recovery (BCDR)	27%
Reactie op incidenten	27%
Endpointdetectie en respons	25%
Geautomatiseerde patching van software	25%
Platform voor mobiel beheer	23%
Threat hunting	20%
Pentesting	14%
Forensisch onderzoek	12%

Slechts 43% van de respondenten geeft trainingen op het gebied van beveiligingsbewustzijn.

MKB's zijn klaar om te investeren in de cloud

De toename van cybercriminaliteit in de afgelopen jaren heeft ertoe geleid dat bedrijven bereid zijn te investeren in cloudbeveiliging.

De belangrijkste aandachtsgebieden voor IT-beveiliging waar MKB's de komende 12 maanden in willen investeren

Investeringsgebied	Reactie
Netwerkbeveiliging	47%
Cloudbeveiliging	45%
Cyberverzekering	36%
Beveiliging van e-mail-/samenwerkingstools	29%
Endpoint-beveiliging	27%
Beoordeling van kwetsbaarheden	26%
Business Continuity and Disaster Recovery (BCDR)	25%
Weet ik niet	5%

Netwerkbeveiliging en cloudbeveiliging zijn de belangrijkste gebieden waarin in 2023 zal worden geïnvesteerd.

Cyberbedreigingen

MKB's hebben een breed scala aan beveiligingsproblemen

Een blik achter de schermen op de factoren, die MKB's als schuldigen voor hun beveiligingsproblemen aanwijzen, kan u helpen hun pijnpunten met vertrouwen tegemoet te treden.

De belangrijkste redenen waarom MKB's vinden dat ze problemen met cyberbeveiliging hebben gehad

Probleem	Reactie
Phishing-e-mails	37%
Kwaadaardige websites/webadvertenties	27%
Zwakke wachtwoorden/slecht toegangsbeheer	24%
Slechte gebruikerspraktijken/goedgelovigheid	24%
Gebrek aan training in cyberbeveiliging voor eindgebruikers	23%
Gebrek aan training van beheerders op het gebied van cyberbeveiliging	19%
Phishing-telefoontjes	19%
Gebrek aan verdedigingsmiddelen (antivirus)	19%
Onvoldoende ondersteuning voor de beveiliging van verschillende soorten gebruikersapparaten	18%
Verouderde beveiligingspatches	18%
Gebrek aan fondsen voor IT-beveiligingsoplossingen	17%
Verloren/gestolen werknemersgegevens	17%
Gebrek aan overtuiging van het uitvoerend kader om beveiligingsoplossingen in te voeren	16%
Toegang tot het remote desktop protocol (RDP)	15%
Shadow IT	13%

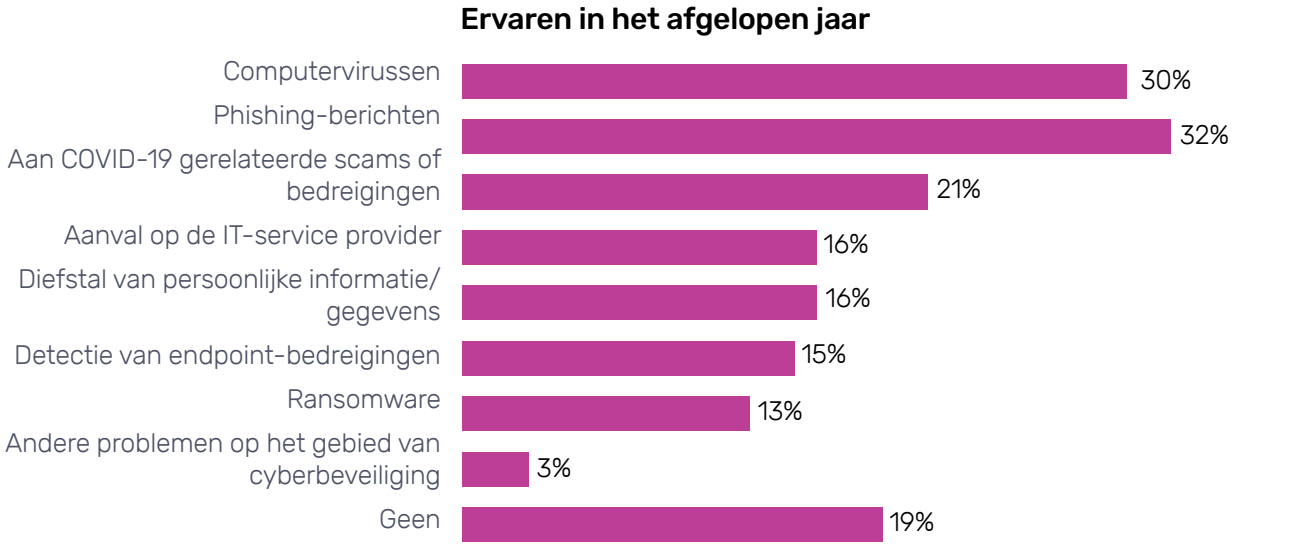
Ongeveer 42% van de MKB's wijten hun beveiligingsproblemen aan een gebrek aan training.

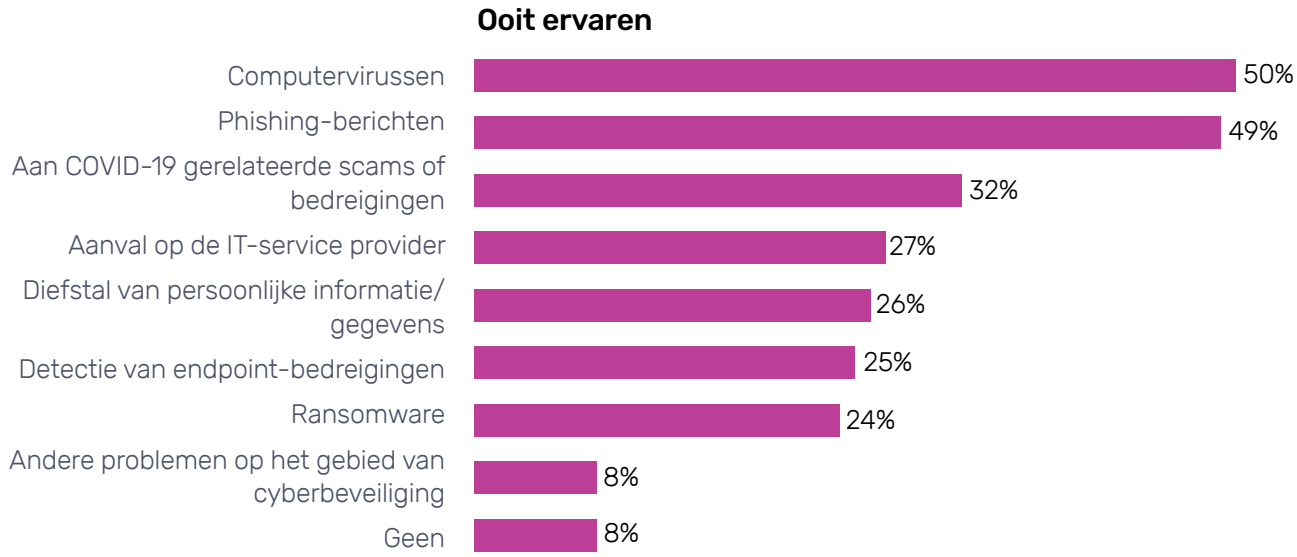
MKB's worden geplaagd door phishing

Veel van onze respondenten zien phishing als de hoofdverdachte voor beveiligingsproblemen, en meer dan een kwart van de respondenten heeft te maken gehad met een aanval op hun IT-service provider (16% in het afgelopen jaar). Dit is een kans voor MSP's om zeer veilige service te bieden.

Problemen op het gebied van cyberbeveiliging die de afgelopen 12 maanden gevolgen hebben gehad voor het MKB.

Bijna een derde van de respondenten had vorig jaar te maken met phishing en virussen.

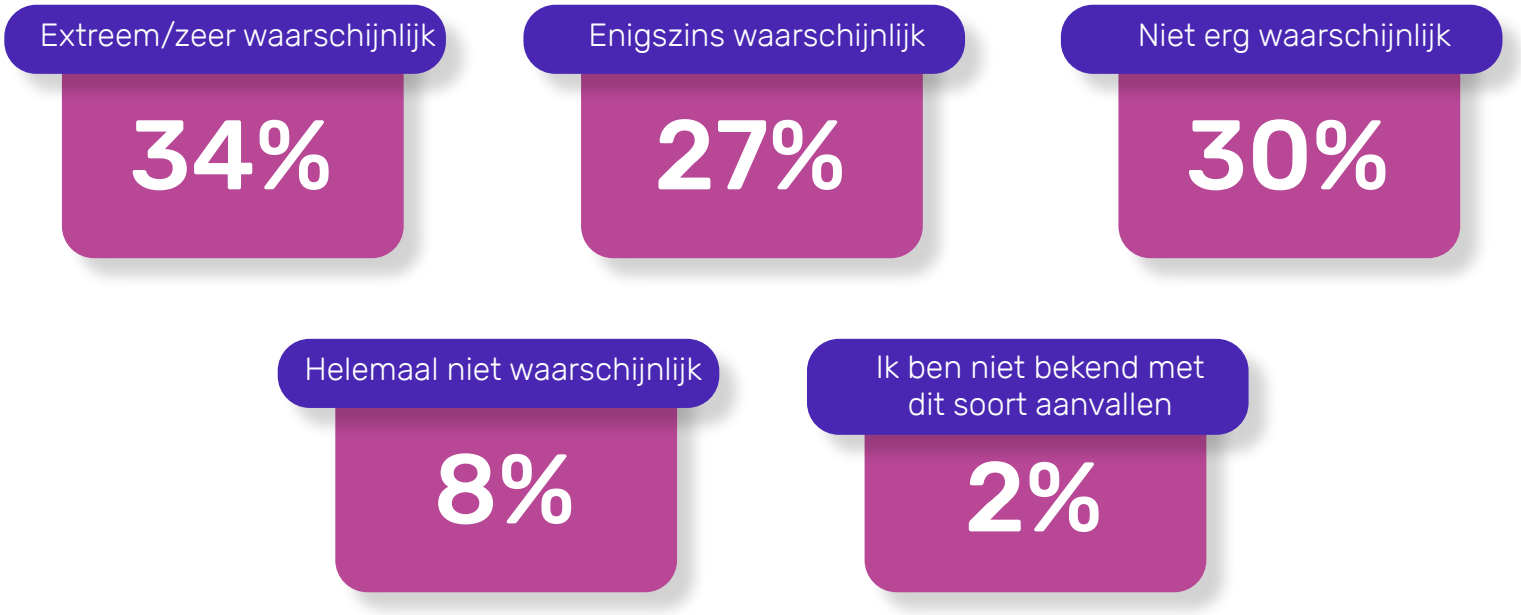




Bijna driekwart van de bedrijven zegt dat een ransomware-aanval een doodsteek voor het bedrijf zou zijn

Bedrijven weten dat een ransomware-aanval hen kan ruïneren, en ze zoeken naar manieren om dit te voorkomen.

Ongeveer 60% van de respondenten denkt dat hun organisatie in de komende 12 maanden kan worden getroffen door een succesvolle ransomware-aanval.



Ongeveer 70% van de MKB's gaf toe dat de impact van een ransomware-aanval extreem of aanzienlijk zou zijn.

Extreme impact – het zou moeilijk zijn om te herstellen

17%

Aanzienlijke impact

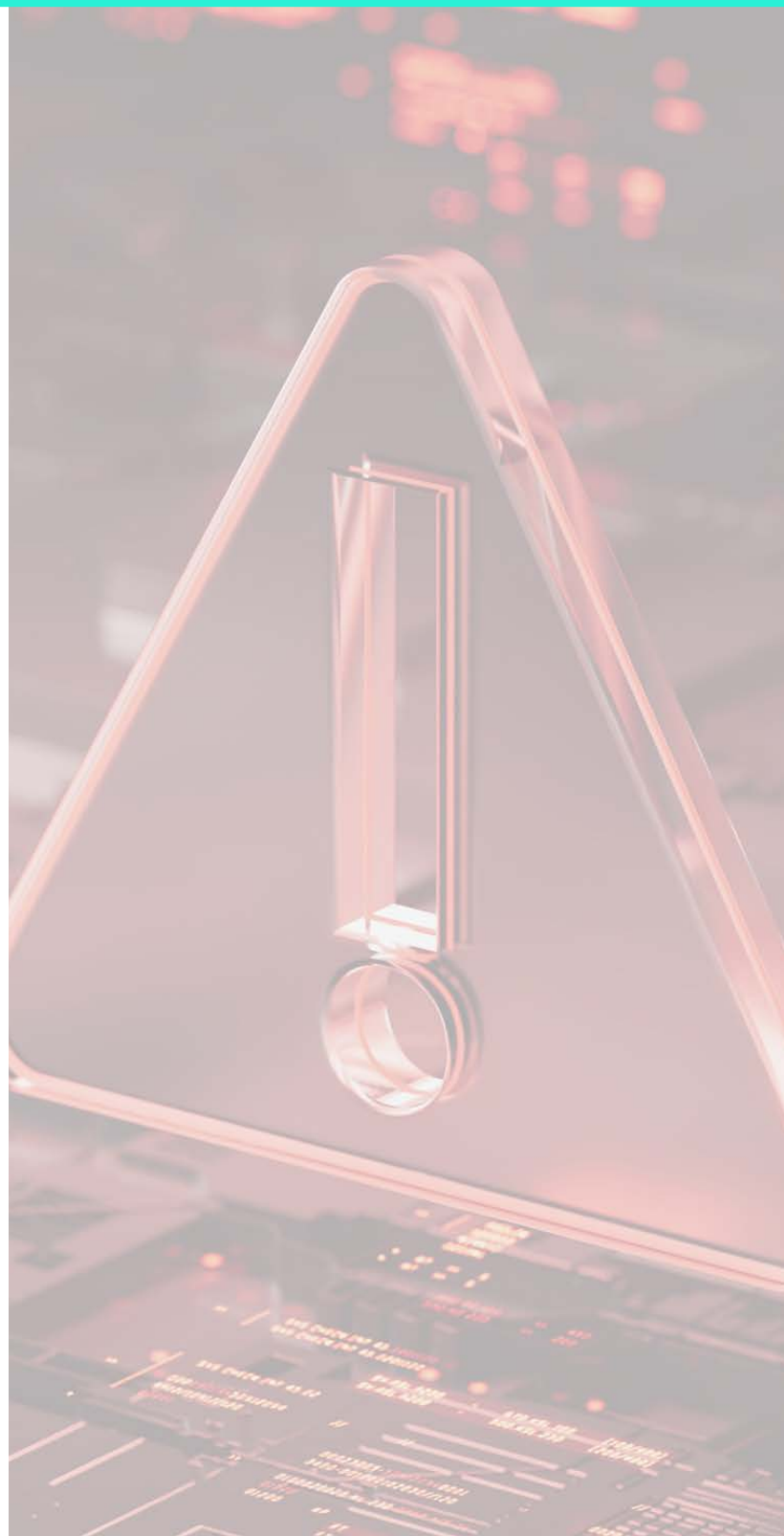
53%

Minimale impact

28%

Geen impact

3%



De eisen voor losgeld lopen sterk uiteen

Als u klanten en potentiële klanten een duidelijk beeld geeft van de eis voor losgeld waarmee zij te maken kunnen krijgen, kan dat hen helpen de werkelijke schade voor hun bankrekeningen te overzien.

Bijna een derde van de MKB's kreeg te maken met 10.000 tot 50.000 dollar aan kosten voor losgeld.

Bedrag van het losgeld	Reactie
Minder dan $ 100	2%
$ 100 tot minder dan $ 500	4%
$ 500 tot minder dan $ 1.000	10%
$ 1.000 tot minder dan $ 5.000	21%
$ 5.000 tot minder dan $ 10.000	25%
$ 10.000 tot minder dan $ 25.000	20%
$ 25.000 tot minder dan $ 50.000	11%
$ 50.000 of meer	6%

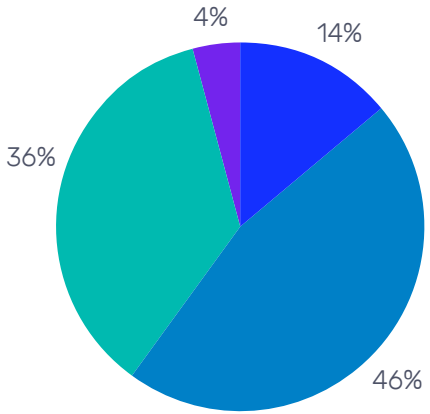
De meeste MKB's verwachten dat ze een keer worden gephisht

Iets minder dan driekwart van de respondenten denkt dat het waarschijnlijk is dat hun organisatie het komende jaar met een phishing-aanval te maken krijgt, en ook hier zijn ze op zoek naar manieren om dat risico te beperken.

Ongeveer 72% van de respondenten verwacht het komende jaar een phishing aanval.

Waarschijnlijkheid	Reactie
Extreem/zeer waarschijnlijk	41%
Enigszins waarschijnlijk	31%
Niet erg waarschijnlijk	22%
Helemaal niet waarschijnlijk	7%

Meer respondenten dachten dat zij in het komende jaar het slachtoffer zouden worden van phishing dan van ransomware, maar zij dachten dat de impact van een succesvolle ransomware-aanval groter zou zijn voor hun organisatie dan de impact van een phishing-aanval.



Bijna de helft van de respondenten denkt dat een phishing-aanval aanzienlijke gevolgen zou hebben voor hun bedrijf.

- Minimale impact
- Aanzienlijke impact
- Extreme impact – het zou moeilijk zijn om te herstellen
- Geen impact

MKB's hebben vertrouwen in hun vermogen om te herstellen van een incident op het gebied van cyberbeveiliging

Ondanks dit vertrouwen zijn er op dit gebied volop mogelijkheden voor MSP's om nieuwe oplossingen voor te stellen om risico's te beperken of om de beveiliging van een klant of prospect te upgraden om deze nog sterker te maken – 16% van de respondenten vertelde ons dat hun organisatie gedoemd zou zijn te verdwijnen in geval van een succesvolle cyberaanval of een ander schadelijk cyberbeveiligingsincident, en 47% zei dat herstel moeilijk zou zijn.

Succesvol rampherstel is eenvoudiger gezegd dan gedaan

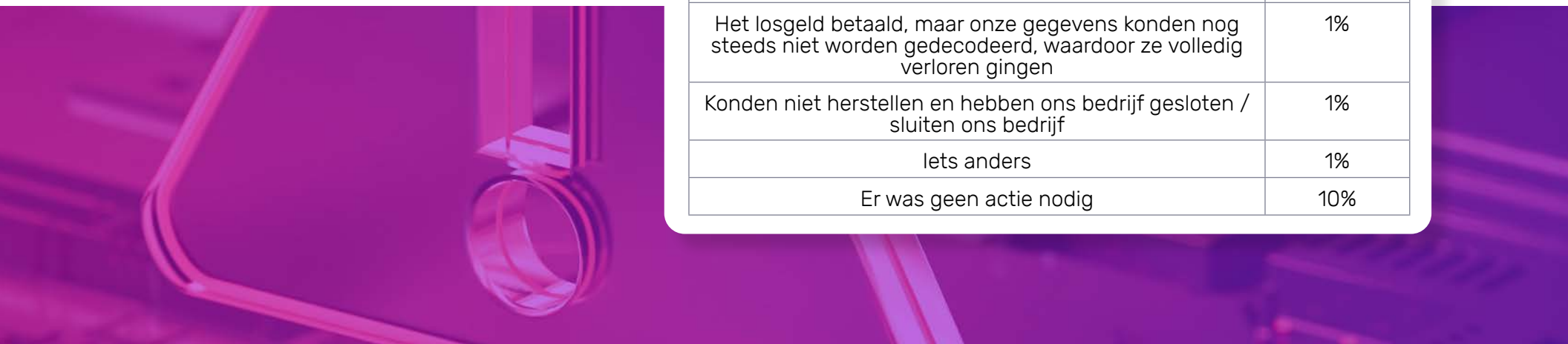
MSP's kunnen MKB's de hulp bieden die ze nodig hebben om hun back-up- en herstelprocessen te verbeteren.

Een vijfde van de respondenten moest alle systemen opnieuw installeren en configureren om weer aan het werk te kunnen.

Iets minder dan de helft van de respondenten (47%) zei dat hun bedrijf waarschijnlijk zal herstellen van een cyberaanval of incident op het gebied van cyberbeveiliging, maar dat het pijnlijk zou zijn.

Resultaat	Reactie
Herstel zou makkelijk zijn	**37%**
Herstel zou moeilijk zijn	**47%**
We zouden het niet overleven	**16%**

Actie ondernomen om terug te keren naar de oorspronkelijke situatie	Reactie
Voerde disaster recovery (DR) uit en herstelde alles vanaf volledige back-ups	30%
Een deel van de systemen hersteld en de rest opnieuw geïnstalleerd en geconfigureerd	29%
Al onze systemen vanaf de grond af opnieuw geïnstalleerd en geconfigureerd	21%
Het losgeld betaald om onze gegevens te decoderen	2%
Het losgeld niet betaald en onze gegevens volledig verloren	2%
Het losgeld betaald, maar onze gegevens konden nog steeds niet worden gedecodeerd, waardoor ze volledig verloren gingen	1%
Konden niet herstellen en hebben ons bedrijf gesloten / sluiten ons bedrijf	1%
Iets anders	1%
Er was geen actie nodig	10%



Downtime kost gemiddeld $ 126.000

Downtime is een duur probleem waar bijna de helft van onze respondenten het afgelopen jaar mee te maken heeft gehad. De zakelijke impact en de hoge kosten van downtime bieden MSP's de mogelijkheid om oplossingen aan te bevelen, zoals BCDR, die de downtime in geval van een beveiligingsincident beperken. De kosten van downtime zijn ook een gegeven dat kan worden gebruikt wanneer wordt gesproken over training in veiligheidsbewustzijn en andere preventieve maatregelen.

$ 126.000 zijn de gemiddelde kosten van de downtime, inclusief gederfde inkomsten.

Kosten van downtime	Reactie
$ 1.000 tot minder dan $ 250.000	84%
$ 1.000 tot minder dan $ 250.000	8%
$ 1.000 tot minder dan $ 250.000	4%
$ 750.000 tot minder dan $ 1 miljoen	3%
$ 1 miljoen of meer	1%

Handmatige back-up is de meest gebruikte herstelmethode

Iets minder dan de helft van de respondenten van de enquête (49%) gaf aan dat hun organisatie bij het laatste incident op het gebied van cyberbeveiliging vertrouwde op handmatige back-ups om gegevens te herstellen. Dat betekent dat de helft van de door ons onderzochte bedrijven moet updaten naar cloudback-up en de voordelen van BCDR moet leren kennen – een grote kans voor MSP's.

De beste oplossingen of methoden om gegevens te herstellen.

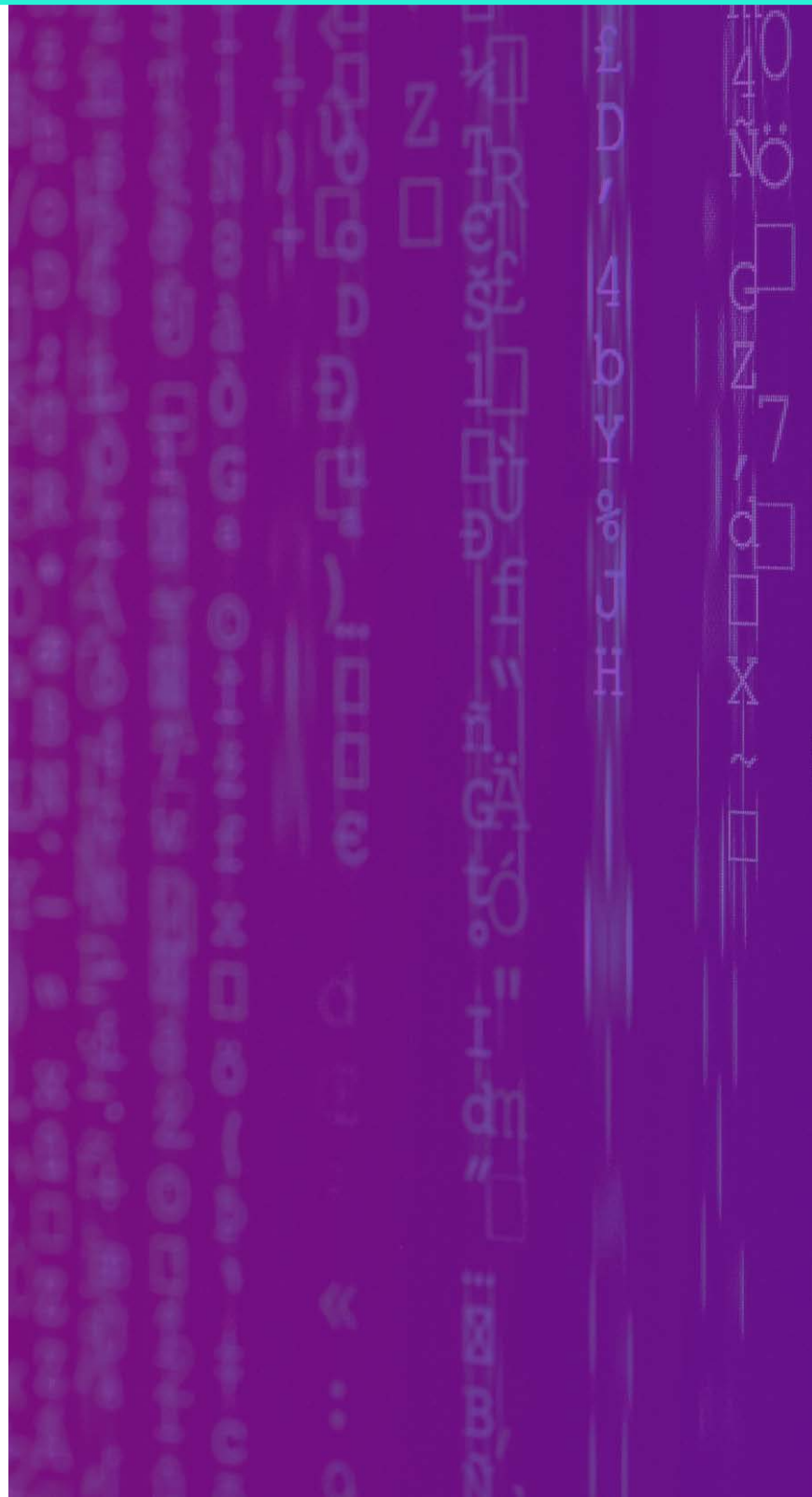
Herstelmethode	Reactie
Handmatige back-up	49%
Kopiëren vanaf oude systemen	36%
Continue beschikbaarheid	36%
BCDR van derden	32%
Iets anders	11%
We hebben niets gedaan en onze gegevens niet hersteld	2%
We hebben geen gegevens verloren	13%

Ongeveer de helft van de MKB's met een probleem op het gebied van cyberbeveiliging was binnen een dag weer operationeel

Tegenwoordig gaat het er niet om óf je een incident hebt, maar wanneer, en oplossingen die de hersteltijd verkorten zullen aantrekkelijk zijn voor bedrijven.

Ongeveer 45% van de bedrijven had meer dan twee dagen downtime.

Hersteltijd	Reactie
Geen – we hadden geen downtime	12%
Minder dan 1 dag	23%
1 dag	20%
2 tot 3 dagen	31%
4 tot 6 dagen	10%
Een week of langer	3%
Weet ik niet	1%
Geef liever geen antwoord	1%



Cyberverzekering

De meeste MKB's hebben of zijn in de markt voor een cyberverzekering

Respondenten met een cyberverzekering voeren waarschijnlijk ook andere slimme beveiligingspraktijken uit. Zij hebben over het algemeen meer IT-ondersteuning, meer kaders voor cyberbeveiliging en meer beveiligingsoplossingen ingezet. Ook is de kans groter dat zij in het verleden een incident op het gebied van cyberbeveiliging hebben meegemaakt.

Bijna driekwart van de respondenten heeft een cyberverzekering.

Een derde van degenen zonder cyberverzekering is zeer waarschijnlijk van plan er in de komende 12 maanden in te investeren.

Heeft u een cyberverzekering?

Ja 69%

Nee 23%

Weet ik niet 8%

Waarschijnlijkheid	Reactie
Extreem/zeer waarschijnlijk	37%
Enigszins waarschijnlijk	38%
Niet erg waarschijnlijk	22%
Helemaal niet waarschijnlijk	4%

Onderzoeksmethode

Het Datto-rapport over cyberbeveiliging voor MSP's in het MKB is samengesteld uit een subset van gegevens die zijn verzameld in een onderzoek onder 2.913 IT-besluitvormers dat in juli en augustus 2022 is uitgevoerd. Respondenten moesten een IT-besluitvormer zijn bij een MKB' met 10 tot 300 werknemers. De voor de analyse gekozen markten waren Noord-Amerika (VS en Canada), het Verenigd Koninkrijk, Duitsland, Nederland, Australië, Nieuw-Zeeland en Singapore.

Over Datto

Datto, een merk van Kaseya, biedt cloud-gebaseerde software- en technologieoplossingen van topkwaliteit die door managed service providers (MSP's) worden geleverd. Datto biedt oplossingen op het gebied van Unified Continuity, Networking en Business Management en heeft een uniek ecosysteem van MSP-partners gecreëerd. Deze partners leveren Datto-oplossingen aan meer dan één miljoen bedrijven over de hele wereld. Sinds de oprichting in 2007 heeft Datto elk jaar prijzen gewonnen voor de snelle groei, de productuitmuntendheid, zijn superieure technische ondersteuning en voor het bevorderen van een uitstekende werkplek. Het hoofdkantoor ligt in Norwalk (Connecticut, VS), maar Datto heeft wereldwijde kantoren in het Verenigd Koninkrijk, Nederland, Denemarken, Duitsland, Canada, Australië, China en Singapore. Meer informatie is te vinden op datto.com.