2022

ESET Mkb Digital Security Sentiment Report

CYBERRISICO'S ZETTEN MKB-BEDRIJVEN AAN TOT IMPLEMENTATIE VAN ENTERPRISE-OPLOSSINGEN

Digital Security

Progress. Protected.

SECURITY OPSCHALEN:

Zullen mkb-bedrijven inzetten op detection en response om de volgende uitdaging in hun beveiligingstraject te overwinnen?

“In het bedrijfsleven staan uitdagingen vaak niet op zichzelf en kan de ene uitdaging weer impact hebben op de andere. Op dit moment is het voor mkb-bedrijven één van de grootste uitdagingen om up-to-date te blijven wat betreft de laatste cyberdreigingen én de technologieën die je daar juist tegen kunnen beschermen – de wereld beweegt zich enorm snel. Het is geen geheim dat de meeste mkb’ers hierin beïnvloed worden door de uitdagingen die zij hebben op het gebied van tijd & resources om op de juiste manier te investeren in securitymaatregelen. Een aantal zaken spelen hierin een grote rol: human resources, de securityvolwassenheid & financieën. Daarnaast spelen ook zakelijke gevolgen die voortvloeien uit sociale, politieke en economische omstandigheden een rol.

Dit jaar zien we een stijging in web- en emaildreigingen, maar ook van detecties in het algemeen. Naar deze detecties dient men te kijken om op deze manier te blijven optimaliseren en vandaag beter beveiligd te zijn dan gisteren. Het mkb bevindt zich in een bijzondere en opmerkelijke positie. Ze kunnen een aanzienlijk aanvalsoppervlak hebben, maar hebben niet altijd de middelen om zichzelf te beschermen.”

Ashley Schut
Head of SMB & MSP bij ESET in Nederland

SECURITY OPSCHALEN:

Voorafgaand aan de COVID-19 pandemie leken de tech-, retail-, telecom- en zelfs de IT-beveiligingssector goed te groeien. Onder die groei verliep de digitalisering rustig. Nieuwe vormen van handel, communicatie, diensten en producten hadden wortel geschoten, maar de volledige omvang en belofte van de digitalisering bleek nauwelijks zichtbaar. COVID-19 heeft de digitalisering een nieuwe impuls gegeven. Er volgde een stormloop om de productiviteit te verhogen en processen te stroomlijnen, terwijl een enorm leger werknemers uitzocht hoe ze op afstand konden werken via cloud-based samenwerkingsplatformen van Zoom tot Microsoft Teams - het niet langer geruisloze werk van de digitalisering werd nieuw leven ingeblazen.

IT-budgetten schommelden, waardoor onze manier van werken, handelen en winkelen veranderde. Tegelijkertijd leek de business case om serieus werk te maken van bescherming een nieuwe trend in gang te zetten bij kleine en middelgrote ondernemingen om zowel cloud app protections als de meer geavanceerde detection & response-technologie te overwegen. De jaren 2020 tot 2022 leverden zeker genoeg motivatie op – denk aan de Kaseya-, Microsoft Exchange- en Emotet-aanvallen, evenals de vele web-based aanvallen, die zich bij de bestaande zorgen rond ransomware voegden.

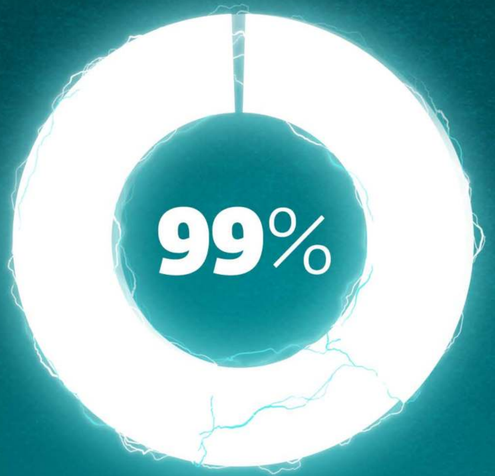
SECURITY OPSCHALEN:

De huidige tijden hebben de zaken nog ingewikkelder gemaakt, zelfs buiten de beruchte personeelskrapte, het chiptekort en the Great Resignation om – zij hebben de oorlog in Oekraïne in het wereldwijde nieuws gebracht, waarbij Europese media dit als een extra vector voor cyberaanvallen aanhaalden. Centraal in de berichtgeving staan dreigingen die zowel gericht zijn op verstoring van het bedrijfsleven als op het verwezenlijken van staatsdoeleinden.

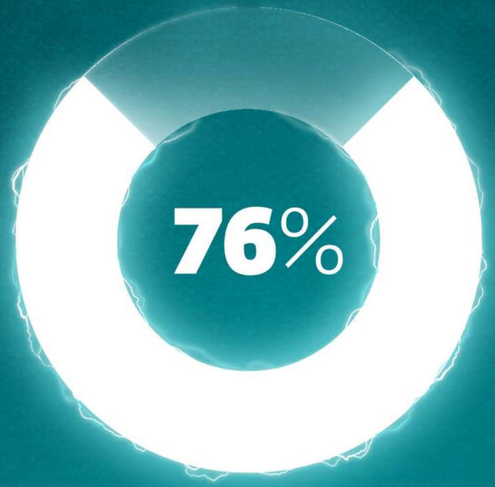
Hoewel alle bedrijven met deze en tal van andere beveiligingsuitdagingen worden geconfronteerd, moeten kleine en middelgrote ondernemingen in het algemeen proberen ze aan te pakken vanuit de positie van de underdog. Dit zou kunnen worden gezien als een weerspiegeling van de verwachte wendbaarheid en ondernemersgeest van een mkb'er, maar glimpsen van de vluchtige post-COVID-19-economie hebben de behoefte aan doelgerichte en schaalbare digitale beveiliging doen toenemen.

De 2022 Mkb Cybersecurity Survey onderzoekt het sentiment van mkb'ers op dit kruispunt van personele middelen, technische volwassenheid en financiële stress. Laten we eens bekijken hoe deze gebeurtenissen en beveiligingsontwikkelingen het cybersecuritysentiment dat we in onze enquête onder mkb'ers in 2022 hebben ontdekt, opnieuw hebben vormgegeven.

HET MKB IS DE RUGGENGRAAT VAN DE WERELDECONOMIE



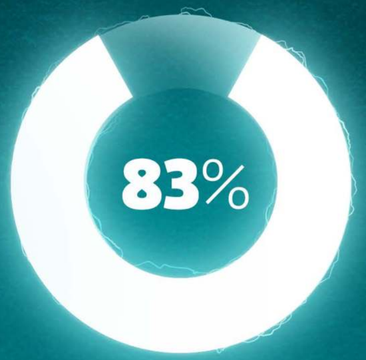
van alle bedrijven in Europa en Noord-Amerika zijn mkb-bedrijven



van het mkb gelooft in de **technologische vooruitgang die hun groei mogelijk maakt**

MKB'ERS STAAN VOOR UITDAGINGEN BIJ HET BESCHERMEN VAN HUN ORGANISATIE, ZOALS OOK BENOEMD IN DE LAATSTE ESET THREAT REPORTS

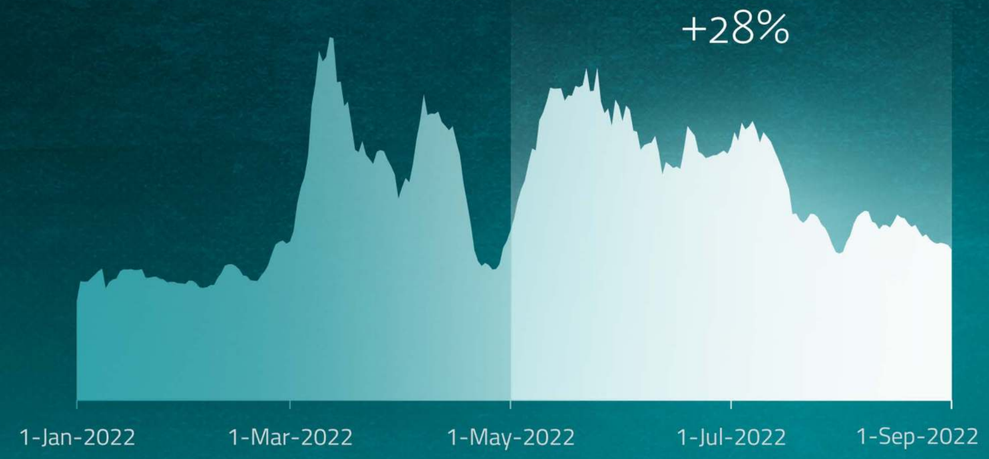
20% meer detecties van cyberdreigingen



van het mkb gelooft dat **cyberoorlog een zeer reële dreiging** is die iedereen kan treffen

HET MKB WORDT GECONFRONTEERD MET EEN STIJGING IN WEB- EN E-MAILDREIGINGEN

Enkele van de meest beruchte aanvalsvectoren voor de levering van malware zijn het web en e-mail. Mkb'ers kunnen toekomstige beveiligingsinspanningen prioriteren om hun zakelijke samenwerkingstools en -toepassingen te beschermen.



28% toename van webdreigingen

66% toename van Outlook login phishing-formulieren verzonden via e-mail

CYBERSECURITY-SENTIMENT BINNEN HET MKB

Mkb'ers zien veel cyberbeveiligingsrisico's en -dreigingen, maar hebben onvoldoende vertrouwen in hun vermogen om met alles om te gaan. Men maakt zich bijvoorbeeld zorgen over werknemers die in aanraking komen met malware, vooral via web-based aanvallen, hoewel ransomware-aanvallen en beveiligingsproblemen bij derden, zoals bij hun leveranciers, op de tweede plaats komen.

Belangrijkste zorgen op het gebied van cybersecurity in de komende 12 maanden

CYBERSECURITY-SENTIMENT BINNEN HET MKB

Waardoor worden deze zorgen gevoed? Het is misschien verrassend dat mkb-bedrijven het gebrek aan bewustzijn omtrent cybersecurity bij hun werknemers als belangrijkste oorzaak zien. Dit is nog belangrijker dan factoren als de gevolgen van de oorlog in Oekraïne en de voortdurende regelingen voor remote werken na COVID-19. Beide hebben geleid tot een toename van de investeringen in cybersecurity bij veel mkb-bedrijven – duidt dit erop dat "cybersecurity al geregeld is" en dus als minder belangrijk voor het digitale bewustzijn wordt gezien?

TOP 5 factoren die het risico op een cyberaanval vergroten volgens het mkb:

85%
Gebrek aan cybersecurity awareness bij werknemers

80%
Een wildgroei van verschillende toepassingen die door werknemers worden gebruikt

79%
Gebruik van Remote Desktop Protocol

78%
Blijvend hybride- of thuiswerken

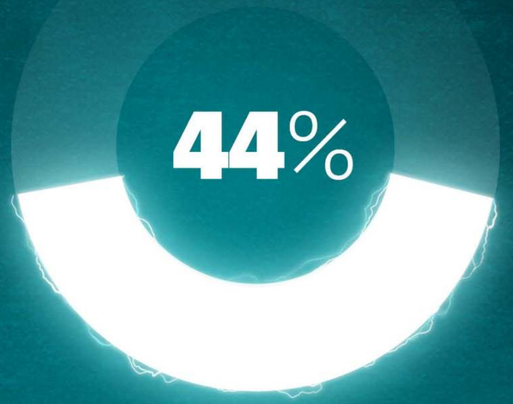
74%
Aanvallen door statelijke actoren als gevolg van de oorlog in Oekraïne

CYBERSECURITY-SENTIMENT BINNEN HET MKB

In ieder geval zien mkb'ers dat er meer te doen is. De belangrijkste uitdagingen op dit moment zijn het bijhouden van de nieuwste cyberdreigingen en de beveiligingstechnologieën om deze tegen te gaan. Maar het overwinnen van deze uitdagingen vereist budget – een uitdaging op zich.

Hoe zullen bedrijven hun budget prioriteren met de economische verschuivingen na COVID-19 en een aanhoudende oorlog in Europa? Misschien ken je het spreekwoord: het piepende wiel krijgt het vet.

Cyberrisico is als een piepend wiel. Zelfs als je niet wilt investeren in betere cyberweerbaarheid, kan een ongewenste golf van cyberaanvallen de begrotingsplannen verstoren.

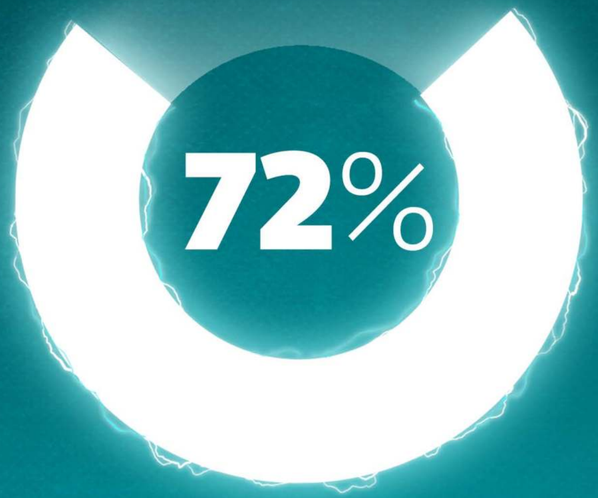


Budgetbeperkingen / gebrek aan investeringen in cybersecurity behoren tot de top drie van cybersecurity-uitdagingen binnen de IT-afdelingen van het mkb

KLEINE EN MIDDELGROTE ONDERNEMINGEN VOELEN ZICH OOK KWETSBAARDER DAN ENTERPRISE-ORGANISATIES...

En als van alle bedrijven het mkb van mening is dat het door zijn omvang kwetsbaarder is voor cyberaanvallen dan enterprise-organisaties, dan betekent dit dat zij het piepende wiel van het cyberrisico harder horen.

72% van de mkb'ers gelooft dat bedrijven van hun omvang kwetsbaarder zijn voor cyberaanvallen dan enterprise-organisaties.



KLEINE EN MIDDELGROTE ONDERNEMINGEN VOELEN ZICH OOK KWETSBAARDER DAN ENTERPRISE-ORGANISATIES...

Het mkb ziet met name de grootste risico's in incidenten die leiden tot verlies van gegevens of ernstige financiële gevolgen. Deze risico-inschatting lijkt terecht. In het afgelopen jaar kreeg tweederde van de mkb-bedrijven te maken met een gegevensbeveiligingsincident dat in de meeste gevallen tot drie maanden duurde om te onderzoeken, wat de mkb'ers aanzienlijke kosten opleverde. De totale geschatte kosten van organisaties na een inbreuk bedroegen (globaal gezien) gemiddeld bijna 220.000 euro en volgens de Nederlandse respondenten bijna 270.000 euro - geen gering bedrag.

Mkb-bedrijven zijn het meest bezorgd over onderstaande gevolgen van een cyberaanval

74%
Financiële impact

62%
Gegevens kwijtraken

53%
Het vertrouwen van klanten kwijtraken

51%
Verstoring van de bedrijfsvoering

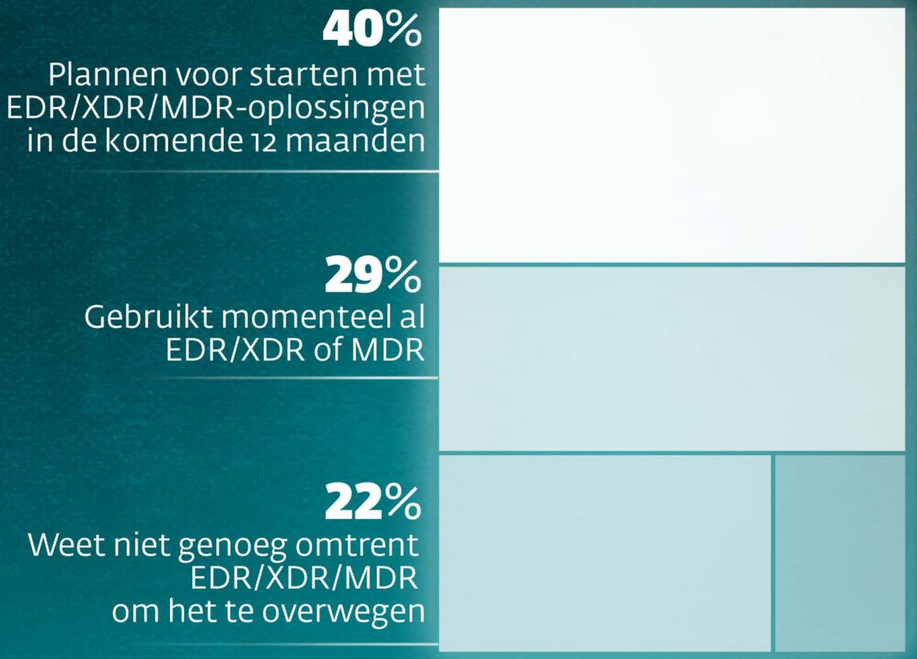
46%
Imagoschade

EEN GROEIENDE BEHOEFTE?

De typische reactie na dergelijke incidenten is om te investeren in opleiding voor het IT-team, wat geen verrassing is, aangezien het lage niveau van cybersecurity awareness van werknemers de belangrijkste oorzaak is van de bezorgdheid van het mkb. Maar veel mkb'ers reageren ook door een audit uit te voeren of nieuwe cyberbeveiligingsinstrumenten aan te schaffen.

Schokkend is de enorme vraag naar detection en response-oplossingen. Deze worden traditioneel alleen door grotere organisaties gebruikt om diep inzicht in hun netwerken te krijgen en de hoofdoorzaak van cyberincidenten vast te stellen. Met een dergelijke mogelijkheid zou een mkb-bedrijf direct de uitdaging aangaan om de nieuwste cyberdreigingen het hoofd te bieden met een innovatieve tool van enterprisekwaliteit.

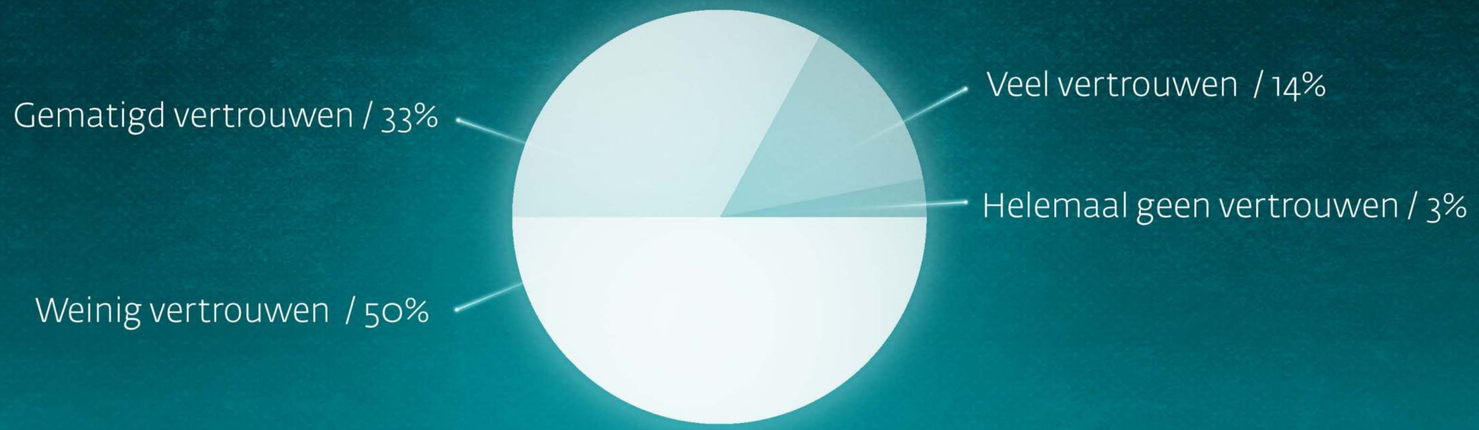
Implementatie van EDR/XDR/MDR oplossingen



EEN GROEIENDE BEHOEFTE?

Het is geen verrassing dat minder dan de helft van de mkb'ers aangeeft een matig tot groot vertrouwen te hebben in hun cyberweerbaarheid. Dit komt onder meer door de bezorgdheid over de interne cybersecuritykennis, de toegang tot third-party experts en de slechte responstijden bij incidenten.

Algemeen vertrouwen in cyberweerbaarheid voor de komende 12 maanden blijft laag



Slechts **47%** van de mkb'ers zegt matig/zeer veel vertrouwen te hebben in in hun cyberweerbaarheid

EEN GROEIENDE BEHOEFTE?

Toen echter werd gevraagd naar complexe IT-beveiligingsprocessen zoals forensisch onderzoek naar dreigingen, sprak 64% een groot vertrouwen uit, hoewel minder dan 30% van de Nederlandse respondenten aangaf gebruik te maken van producten voor detection en response op endpoints zoals EDR. Dit contrast wijst mogelijk op overmoedigheid of op de behoefte aan een beter begrip van wat de weg naar detection en response biedt.

Mkb'ers hebben het meeste vertrouwen in de volgende gebieden:

76%
Zekerheid in hun IT-team op het gebied van cybersecuritykennis

76%
Toegang tot cybersecurity-experts van buitenaf

71%
Snelheid waarmee zij kunnen identificeren, isoleren en reageren op een dreiging

Het is bijna een kip-en-ei scenario. Mkb'ers erkennen de waarde van forensisch onderzoek naar dreigingen en denken inderdaad gebruik te kunnen maken van detection and response. Tegelijkertijd is het feitelijke gebruik van deze tools door het mkb relatief laag en vereist het een voldoende hoog niveau van securityvolwassenheid door IT-teams en een bereidheid om te investeren die veel mkb'ers eenvoudigweg niet hebben laten zien.

Uiteindelijk blijkt uit de benchmarking van de ESET 2022 Mkb Cybersecurity Survey dat er behoefte is aan een effectieve cybersecuritystrategie, één die gaten kan dichten en verbeterde cyberweerbaarheid kan leveren. Wanneer deze reis intelligent en geschaald gebruik van endpoint detection en response omvat, kan jouw onderneming haar vertrouwen vergroten en zich weer richten op kerncompetenties, groei en innovatie.

"IT-dienstverleners, zoals Managed Service Providers (MSPs), kunnen én moeten hier een cruciale rol in spelen – zij kunnen met hun expertise zorgen voor de juiste resources en meer schaalbare oplossingen voor het mkb, door deze te verwikkelen in hun dienstverlening om op deze wijze hoogwaardige securitydiensten te leveren. MSPs hebben de mogelijkheid om mkb'ers op grote schaal te beveiligen – maar ook de technologie op de juiste manier in te zetten en te benutten.Mkb'ers geloven in de technologische vooruitgang die hun groei mogelijk maakt – en ESET is er om de technologie die deze vooruitgang mogelijk maakt te beschermen."

Ashley Schut, Head of SMB & MSP bij ESET in Nederland

Wij hopen dat dit rapport veel belangrijke vragen heeft opgeworpen en dat het je heeft geholpen om beter te bepalen waar je met jouw organisatie naartoe wilt.

Digital Security
Progress. Protected.

Voor media-aanvragen kun je contact opnemen met
Saranda Walgaard via saranda.walgaard@eset.nl

Voor vragen omtrent de trends in het mkb-segment kun je contact opnemen met
Ashley Schut via ashley.schut@eset.nl