datto

Datto's rapport over de wereldwijde stand van zaken op het gebied van Channel Ransomware

Volg ons op: Twitter, Instagram, Facebook, LinkedIn, YouTube

Inschrijven voor ons blog: www.datto.com/blog

Inhoudsopgave

Inleiding

Datto's rapport over de wereldwijde stand van zaken op het gebied van Channel Ransomware bestaat uit statistieken die uit een enquête zijn gehaald die onder meer dan 1.000 managed service providers (MSP's) over heel de wereld is gehouden. Het rapport biedt een uniek inzicht in de stand van zaken van ransomware vanuit het oogpunt van het IT-kanaal en hun klanten uit het midden- en kleinbedrijf (MKB) die dagelijks met deze besmettingen te maken hebben. Het rapport biedt een schat aan details over ransomware, waaronder de trends, frequentie, doelen, impact en aanbevelingen ten opzichte van het jaar ervoor om in het licht van deze toenemende dreiging voor herstel en continuïteit te zorgen.

Ten aanzien van het huidige klimaat gaat het rapport ook in op de impact die COVID-19 en de toename van werken op afstand en cloud computing hebben op de trends in ransomware.

Het doel van dit rapport is een licht te werpen op het huidige landschap van cybersecurity waar bedrijven mee te maken hebben. Bij Datto zijn we van mening dat het midden- en kleinbedrijf met de juiste technologie alles kan bereiken. Wij hopen dat de hier bijeengebrachte informatie MSP's in staat stelt hun klanten te onderwijzen en met hen samen te werken om de risico's in verband met ransomware voor bedrijven te beperken.

Belangrijkste bevindingen

1 **Ransomware is nog steeds de nummer één malwarebedreiging.** Bijna 70% van MSP's ransomware noemt als de meest voorkomende bedreiging voor het MKB.

2 **COVID-19 heeft een impact op beveiliging**—maar niet zo veel als dat u zou denken. MSP's waren verdeeld over de impact die de wereldwijde pandemie op de beveiliging heeft gehad.

3 **Er bestaat nog steeds een kloof tussen MSP's en het MKB op het gebied van ransomware.** 84% van MSP's is 'erg bezorgd' over ransomware, maar slechts 30% meldt dat hun klanten daar net zo over denken.

4 **Het MKB is niet het enige doelwit.** 95% van MSP's is het erover eens dat hun eigen bedrijven steeds meer het doelwit van aanvallen zijn.

5 **Phishing-e-mails staan bovenaan de vectorlijst met geslaagde aanvallen.** Gebrek aan opleiding in cybersecurity, zwakke wachtwoorden en slechte praktijken van gebruikers zijn voorbeelden van andere belangrijke oorzaken van ransomware.

6 **Er is niets moois aan de nasleep van een aanval.** 62% van de MSPs vertelden dat de aanvallen de productiviteit beïnvloedden en 39% vertelden dat hun klanten bedreigende downtime ervaarden.

7 **Het gemiddelde losgeld dat door hackers werd geëist, bleef min of meer gelijk vergeleken met het jaar ervoor.** MSP's melden dat het gemiddelde geëiste losgeld voor het MKB $ 5.600 per incident bedroeg. Vorig jaar was dat $ 5.900.

8 **MSP's melden dat de gemiddelde kosten van uitvaltijd 94% hoger zijn dan in 2019.** De kosten door uitvaltijd zijn bijna 50 keer hoger dan het in 2020 gevraagde losgeld.

9 **91% van MSP's meldt dat klanten met BCDR-oplossingen** minder kans lopen op aanzienlijke uitvaltijd tijdens een aanval met ransomware.

10 **92% van MSP's voorspelt dat aanvallen met ransomware**in het huidige tempo of sneller zullen doorgaan.

COVID-19 en beveiliging

Van alles wat

Veel MSP's vertelden dat het aantal aanvallen met ransomware en de kwetsbaarheden van beveiliging is toegenomen tijdens COVID-19, vanwege de toename in werken op afstand en cloud computing. Er moet echter gezegd worden dat het niet om een overweldigende stijging ging—er is min of meer een gelijke verdeling tussen personen die wel een toename en personen die geen toename zagen.

59%
van MSP's zegt dat het werken op afstand door COVID-19 in meer aanvallen met ransomware heeft geresulteerd.

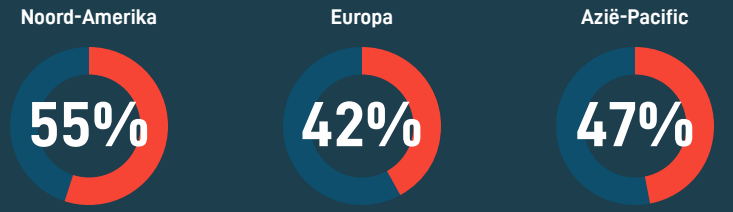
52%
van MSP's meldde dat de verschuiving van de werkbelasting van klanten naar de cloud met een grotere kwetsbaarheid van beveiliging gepaard is gegaan.

Het grotere risico kan volgens de respondenten worden toegeschreven aan onzorgvuldigheid van gebruikers en kwetsbaarheden die met BYOD te maken hebben. "Het risico komt door gebruikers die minder op hun hoede zijn en er zijn nog veel meer dingen die zijn veranderd—gezondheidsrisico's, thuis werken etc.", aldus één MSP.

"[Persoonlijke apparaten] zijn ondanks bezwaren in bedrijfsomgevingen geïntroduceerd: beveiligingsbeleid/eindpuntbescherming etc. Daarnaast zijn er aanzienlijk meer bedreigingen voor de veiligheid door werken op afstand, van diefstal van het apparaat tot gezinsleden die bedrijfsmachines voor persoonlijk werk/studie gebruiken", zegt een ander.

MSP's noemen gezondheidszorg als de meest kwetsbare sector tijdens de pandemie (59%), gevolgd door financiën/verzekeringen (50%) en de overheid (45%).

GEOGRAFISCHE TRENDS



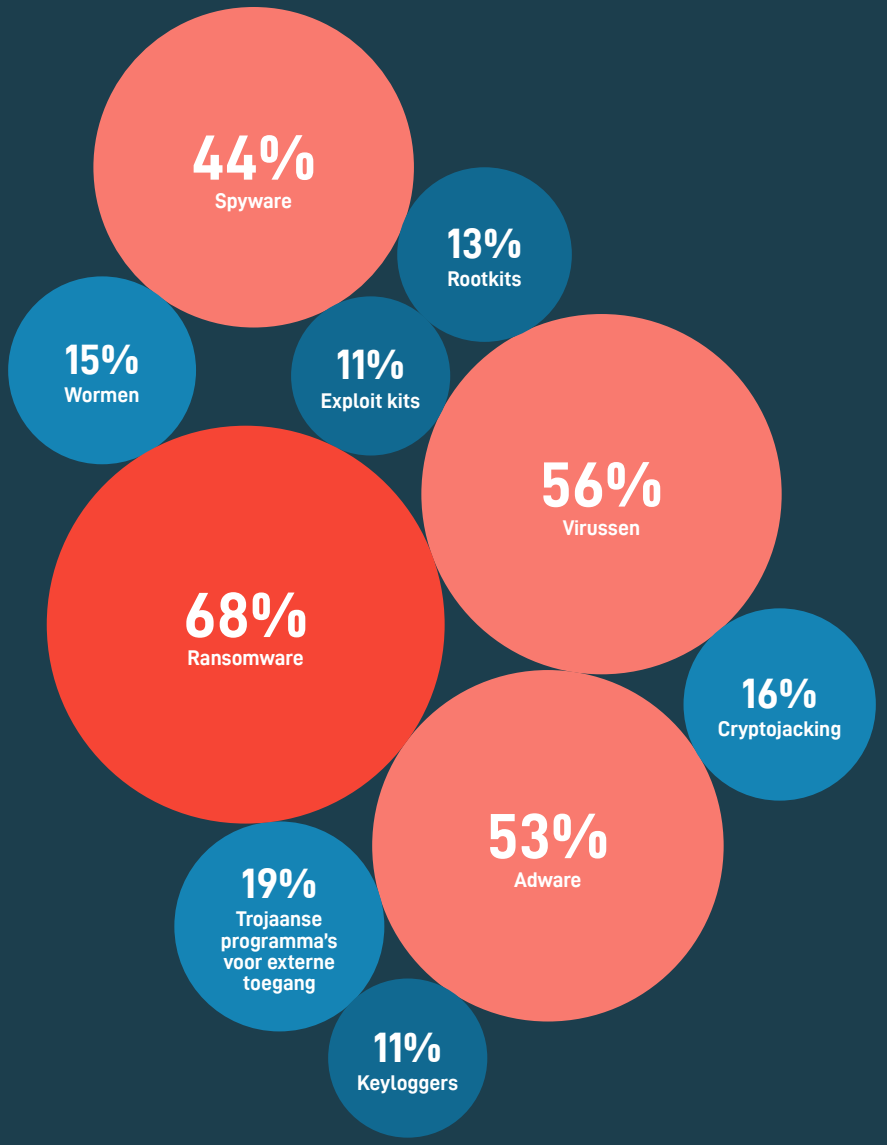
Noord-Amerikaanse MSP's tonen zich iets bezorgder over cloud security dan hun tegenhangers in Europa en Azië-Pacific.

Een veelvoud aan malware heeft het op het MKB gemunt

Bij de malwarebedreigingen die het MKB treffen, voert ransomware nog steeds de lijst aan. Maar het is zeker niet de enige bedreiging. Virussen, adware, spyware en Trojaanse programma's voor externe toegang maken de top vijf compleet.

Cryptojacking, dat het vorig jaar helemaal was, is met 15 procentpunten behoorlijk gedaald. Dit volgt de bevindingen van reguliere rapporten dat cryptojacking minder wordt omdat hackers ongeduldig zijn geworden van de langzame opbrengsten op munt-mijnbouw.

De afgelopen twee jaar hebben MSP's melding gedaan van de volgende soorten malware waar klanten last van hadden:



**Respondenten konden uit meerdere antwoorden kiezen.*

Ransomware is nog steeds een grote uitdaging voor het MKB

Ransomware is nog steeds een plaag voor MSP's en het MKB dat ze bedienen. De respondenten meldden echter dat aanvallen iets minder vaak voorkwamen. 78% van MSP's deed melding van aanvallen op hun klanten tijdens de afgelopen twee jaar, gedaald van 85% vorig jaar. Dat gezegd hebbende, **ransomware is nog steeds een zeer reële bedreiging; 60% van MSP's heeft in de eerste helft van 2020 aanvallen gezien.**

Het is het vermelden waard dat de algemene verstoring door COVID-19 en de daaruit volgende economische terugslag van invloed kan zijn geweest op de frequentie van de aanvallen op het MKB dat MSP's bedienen. Dit is puur speculatie en valt buiten het voor dit rapport uitgevoerde onderzoek. Het wordt interessant om te zien of MSP's een toename in aanvallen met ransomware zullen melden naarmate de internationale economie zich verder herstelt.

MSP's denken dat dit het geval zal zijn. Bijna alle respondenten zeiden dat ze verwachten dat aanvallen met ransomware volgend jaar zullen toenemen.

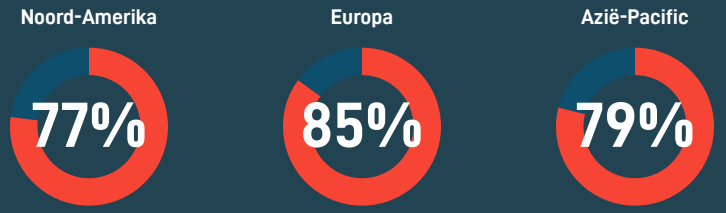
78%
van MSP's doet melding van aanvallen op het MKB tijdens de laatste twee jaar

92%
van MSP's voorspelt dat aanvallen volgend jaar zullen toenemen

60%
van MSP's doet melding van aanvallen op het MKB alleen in 2020

11%
van MSP's meldt dat klanten op één dag meerdere aanvallen kregen te verduren

GEOGRAFISCHE TRENDS



Europese MSP's melden dat hun klanten meer van aanvallen te lijden hadden dan welke andere regio dan ook.

Ransomware gaat niet verdwijnen, maar het kan zijn dat aanvallers hun aandacht tijdelijk naar andere inkomstenstromen hebben verlegd tijdens COVID-19. Als u ransomware ziet als een 'handel' die op veranderende marktomstandigheden moet reageren, dan is het logisch dat die aanvallers zich tijdens een economische neergang op stabielere inkomstenbronnen richten, zoals grotere ondernemingen. Ondernemingen bieden voor hackers een groter 'rendement op de investering' en tonen zich veerkrachtiger bij schommelingen in de economie. Ransomware is een spel van cijfers en grotere bedrijven zijn eenvoudigweg een beter doelwit in moeilijke economische tijden.

Ryan Weeks
Chief Information Security Officer, Datto, Inc.

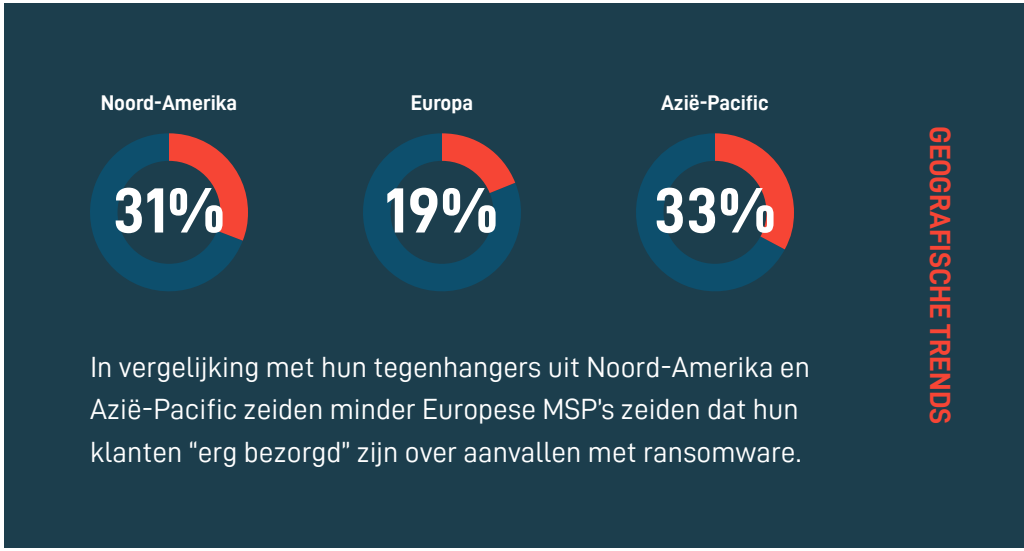
Bewustzijn over ransomware

MKB t.o.v. MSP's

Er bestaat nog steeds een kloof tussen de manier waarop het MKB en MSP's naar ransomware kijken. De meerderheid van MSP's vindt dat bedrijven "erg bezorgd" zou moeten zijn over de bedreiging van ransomware, maar slechts 30% meldt dat hun klanten er net zo over denken. Het lijkt er overigens wel op dat het MKB begint in te zien hoe schadelijk aanvallen met ransomware kunnen zijn. 32% van MSP's meldt dat klanten "matig bezorgd" zijn en 34% zegt dat klanten "enigszins bezorgd" zijn.

30%
van MSP's meldt dat het MKB "zeer bezorgd" is over ransomware

84%
van MSP's meldt dat het MKB "zeer bezorgd" zou moeten zijn over ransomware



Begroting voor beveiliging van MKB neemt toe

50%
van MSP's zegt dat hun klanten de begroting voor IT-beveiliging in 2020 hebben verhoogd.

Afgezien van het grotere bewustzijn, toont de toename in uitgaven voor IT-beveiliging dat het MKB ransomware, en beveiliging in het algemeen, serieus begint te nemen. De lichte afname in aanvallen met ransomware gedurende dit jaar kan er ook op duiden dat deze beveiligingsinspanningen een positieve impact hebben.

Ransomware blijft de inspanningen van cybersecurity omzeilen

Ondanks de hogere uitgaven aan beveiliging melden MSP's dat de inspanningen om aanvallen met ransomware af te wenden, zoals opleiding van werknemers, antivirus, e-mail filteren, pop-upblokkering en eindpunt detectie oplossingen. 50% van hen zei dat ransomware antivirus-/antimalware oplossingen omzeilde.

Wanneer gevraagd om welke antivirus-/antimalware oplossingen het specifiek ging, zeiden MSP's:

59%
Filteren op antimalware (e-mail, netwerk en web)

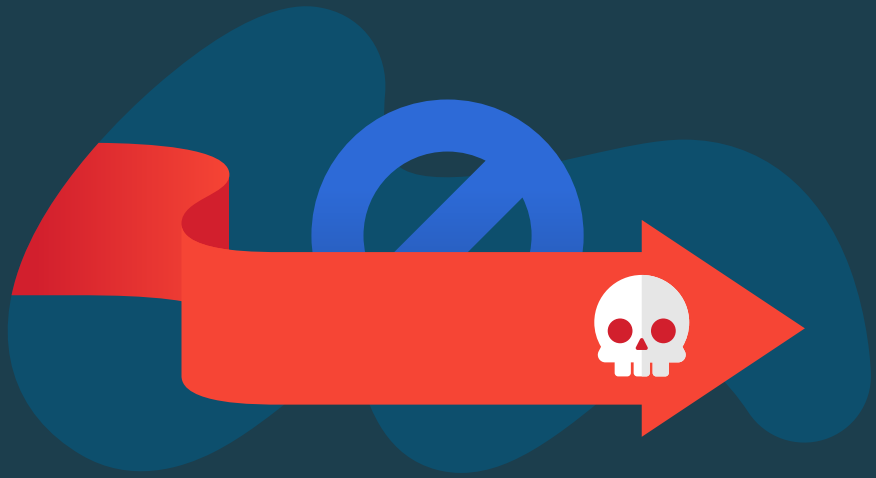
24%
Eindpuntdetectie en reactie

42%
Verouderde antivirus op basis van handtekening

12%
NextGen antivirus

Ransomware kan deze oplossingen omzeilen omdat cybercriminelen vaak hun malware wijzigen om detectie te vermijden. Wat erger is, is dat de social engineering tactieken die criminelen erop na houden om slachtoffers te duperen erg geraffineerd zijn geworden en moeilijk zijn te detecteren—zelfs als klanten over beveiliging zijn voorgelicht (daarover hieronder meer).

Daarom is een meerlaagse benadering tot ransomware met bedrijfscontinuïteit zo belangrijk. Beveiligingssoftware en training zijn essentieel om aanvallen te voorkomen voordat deze plaatsvinden. Bedrijfscontinuïteit stelt organisaties in staat normale activiteiten snel te hervatten als beveiligingsmaatregelen het af laten weten.



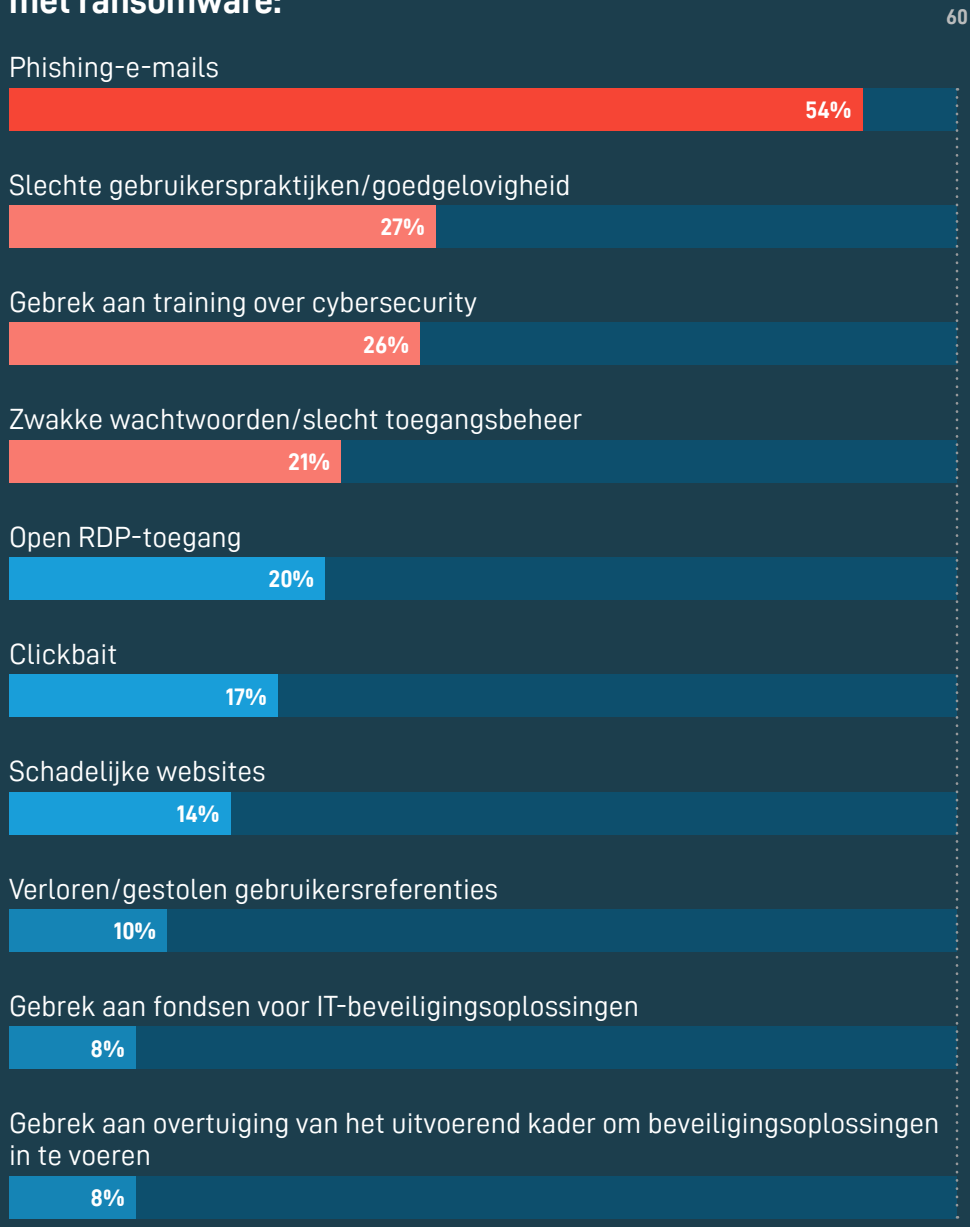
Het MKB blijft toehappen

Zoals al eerder vermeld, is het opleiden van eindgebruikers een essentieel onderdeel van een effectieve strategie voor bescherming tegen ransomware. De resultaten van dit jaars onderzoek zijn daarvan het bewijs: phishing, slechte gebruikerspraktijken en gebrek aan training op het gebied van cybersecurity waren de drie meest voorkomende oorzaken van succesvolle inbreuken door ransomware.

Daarom is het belangrijk dat beveiligingstraining verder gaat dan alleen maar het vaststellen van phishing-aanvallen. Phishing stond weliswaar bovenaan de lijst, maar zwakke wachtwoorden, open RDP-toegang en een hele reeks andere gebruikersfouten waren ook schuld aan inbreuken.

LEZEN 9 tips over cybersecurity die MSP's hun klanten kunnen bieden

Belangrijkste door MSP's gemelde oorzaken van aanvallen met ransomware:



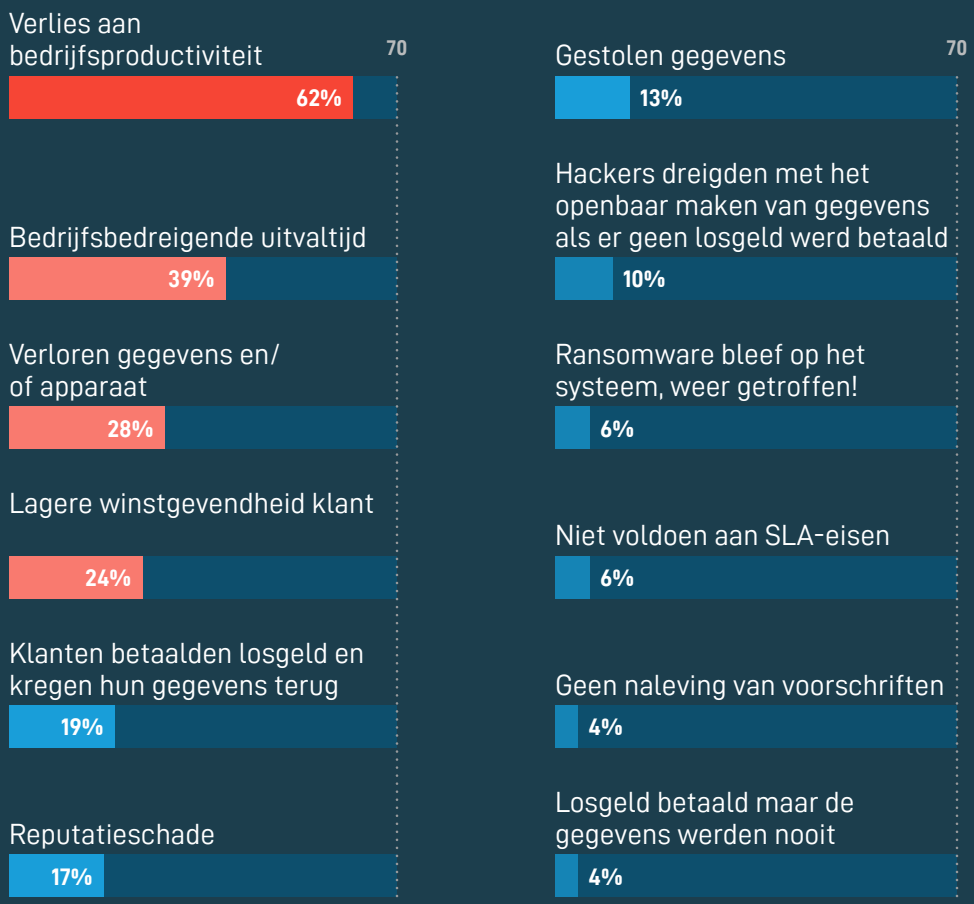
**Respondenten werd gevraagd drie antwoorden te selecteren.*

De nasleep van aanvallen

Aanvallen met ransomware kunnen aanzienlijke uitvaltijd veroorzaken voor bedrijven, omdat breuken zelden tot maar één computer beperkt blijven. Het grootste deel van de ransomware die vandaag de dag in gebruik is, is ontworpen om zakelijke netwerken te verkennen, in de zoektocht om andere machines te besmetten. Als de malware niet wordt gedetecteerd, duurt het niet lang totdat talrijke apparaten, servers en zelfs gegevens in SaaS-toepassingen van gebruikers worden versleuteld. Herstel kan veel tijd in beslag nemen, vooral met traditionele back-uptools.

Daarom is het logisch dat verlies aan bedrijfsproductiviteit en bedrijfsbedreigende uitvaltijd bovenaan de lijst staan met gevolgen van ransomware. Het verklaart ook waarom vrijwel 20% van MSP's meldde dat het MKB werd gedwongen losgeld te betalen om naar normale activiteiten te kunnen terugkeren. Dit alles benadrukt de noodzaak voor een oplossing voor bedrijfscontinuïteit waarmee het MKB snel terug aan het werk kan.

Gevolgen van door MSP's gemelde aanvallen met ransomware:



**Respondenten werd gevraagd drie antwoorden te selecteren.*

Uitvaltijd kost veel meer dan losgeld

Wanneer we het over aanvallen met ransomware hebben, melden MSP's dat **de kosten van uitvaltijd bijna 50 keer hoger zijn dat het geëiste losgeld**.

Gemiddelde losgeld in...

2018	2019	2020
$ 4.300	$ 5.900	$ 5.600

MSP's melden dat de gemiddelde kosten van losgeld in 2020 ongeveer gelijk waren aan die in 2019. Er is dus sprake van een lichte afname in de frequentie van aanvallen, maar hackers eisen nog steeds veel losgeld. Tussen 2018 en 2019 zagen we het gemiddelde losgeld sterk toenemen, toen de geëiste bedragen met 37% stegen.

Gemiddelde kosten voor uitvaltijd in...

2018	2019	2020
$ 46.800	$ 141.000	$ 274.200

MSP's meldden dat de gemiddelde kosten voor uitvaltijd per incident met 94% zijn toegenomen ten opzichte van 2019 en met maar liefst 486% ten opzichte van 2018. Maar wat betekent dit precies? Op het eerste gezicht dat de kosten voor uitvaltijd uiteraard hoger zijn dan twee jaar geleden. Dit kan betekenen dat de kosten voor uitvaltijd zijn toegenomen of dat MSP's er beter in zijn geworden de werkelijke kosten van uitvaltijd te berekenen. Hoe het ook zij, het is duidelijk dat MSP's inzien dat de schade in verband met uitvaltijd in een bedrijf veel meer geld kost dan de het losgeld op zich.

De kosten voor uitvaltijd lopen sterk uiteen van het ene bedrijf op het andere en deze cijfers zijn gebaseerd op schattingen van MSP's. Om de kosten van potentiële uitvaltijd voor uw bedrijf te berekenen, gaat u naar onze Calculator voor hersteltijd en kosten van uitvaltijd.

**Alle antwoorden van de respondenten zijn in Amerikaanse dollars.*

GEOGRAFISCHE TRENDS

2020: Losgeld t.o.v. kosten door uitvaltijd

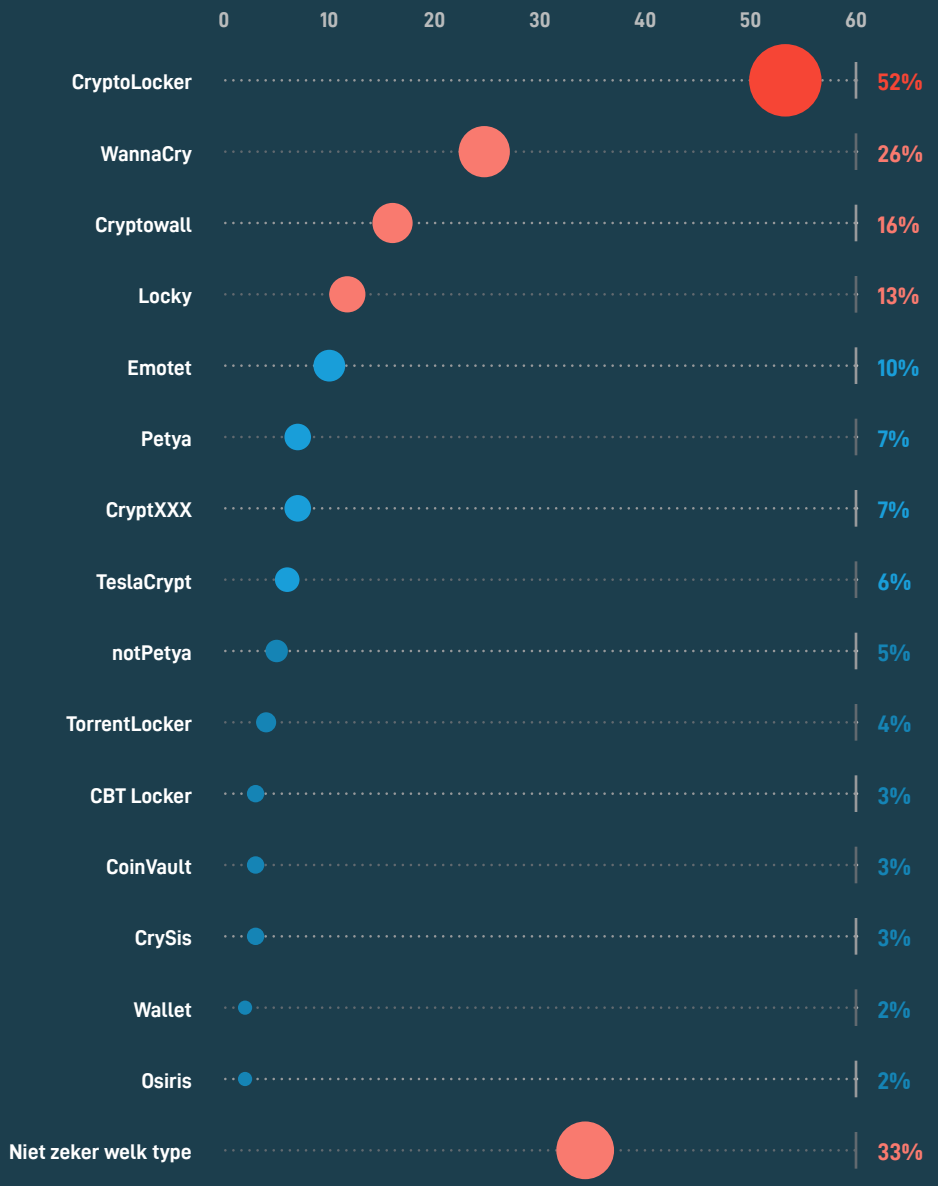
Regio	Losgeld	Uitvaltijd
Noord-Amerika	$ 6.200	$ 308.900
Europa	$ 3.500	$ 185.800
Azië-Pacific	$ 4.400	$ 257.000

Nog steeds vergrendelen (Na al deze jaren)

Voor het vijfde opeenvolgende jaar noemden MSP's CryptoLocker als de belangrijkste variant van ransomware die op hun klanten een impact had (52%). WannaCry was de volgende op de lijst met 26%, gevolgd door Cryptowall (16%) en Locky (13%).

Een saillant detail is dat 33% van de respondenten zei dat ze niet zeker wisten met welke soort ransomware ze te maken hadden. Dit is om twee redenen belangrijk. In de eerste plaats maakt het soort ransomware uiteindelijk niet veel uit—elke soort kan uitvaltijd van een bedrijf tot gevolg hebben. Ten tweede zijn de inspanningen van MSP's in de strijd tegen ransomware en bij het herstel na aanvallen dezelfde.

LEZEN
Veelvoorkomende types ransomware



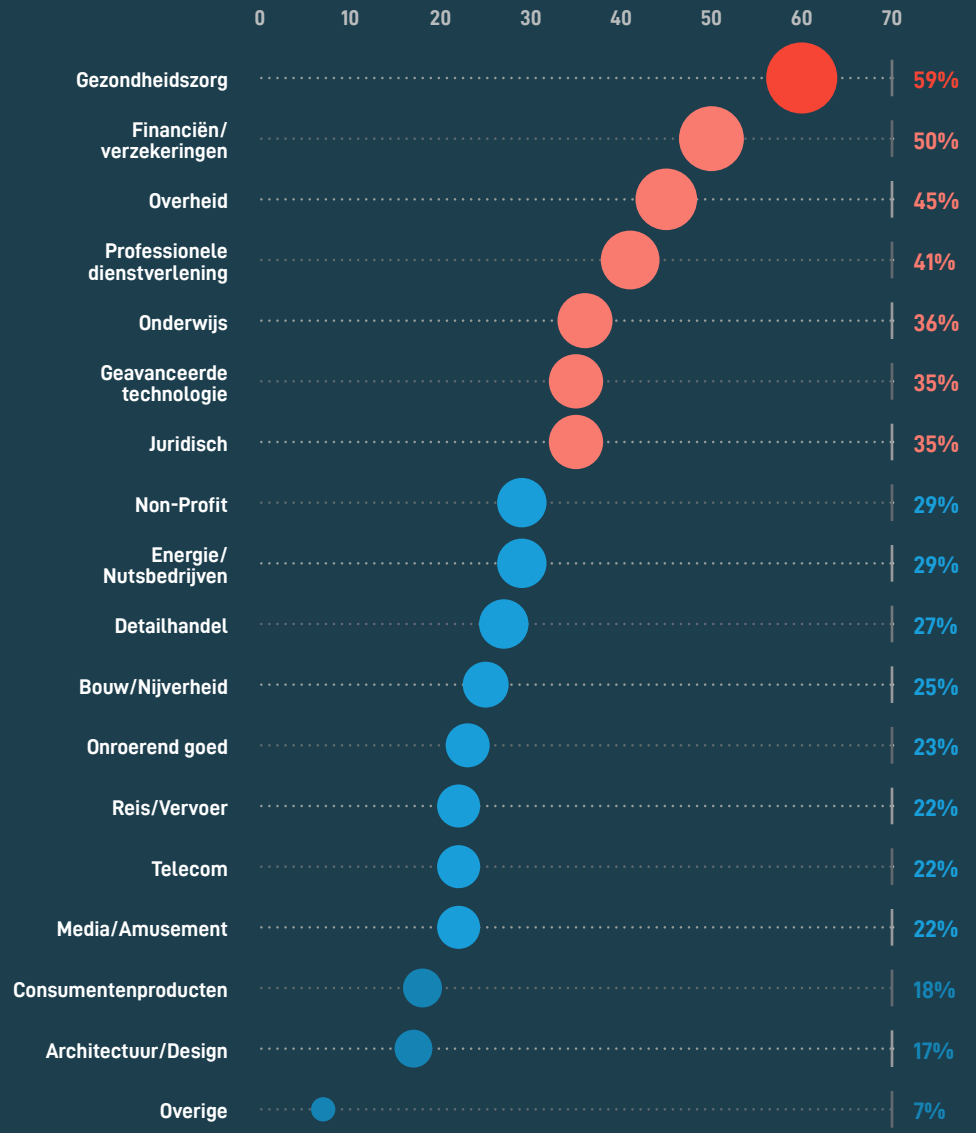
*Respondenten konden uit meerdere antwoorden kiezen.

Meest vatbare sectoren voor ransomware

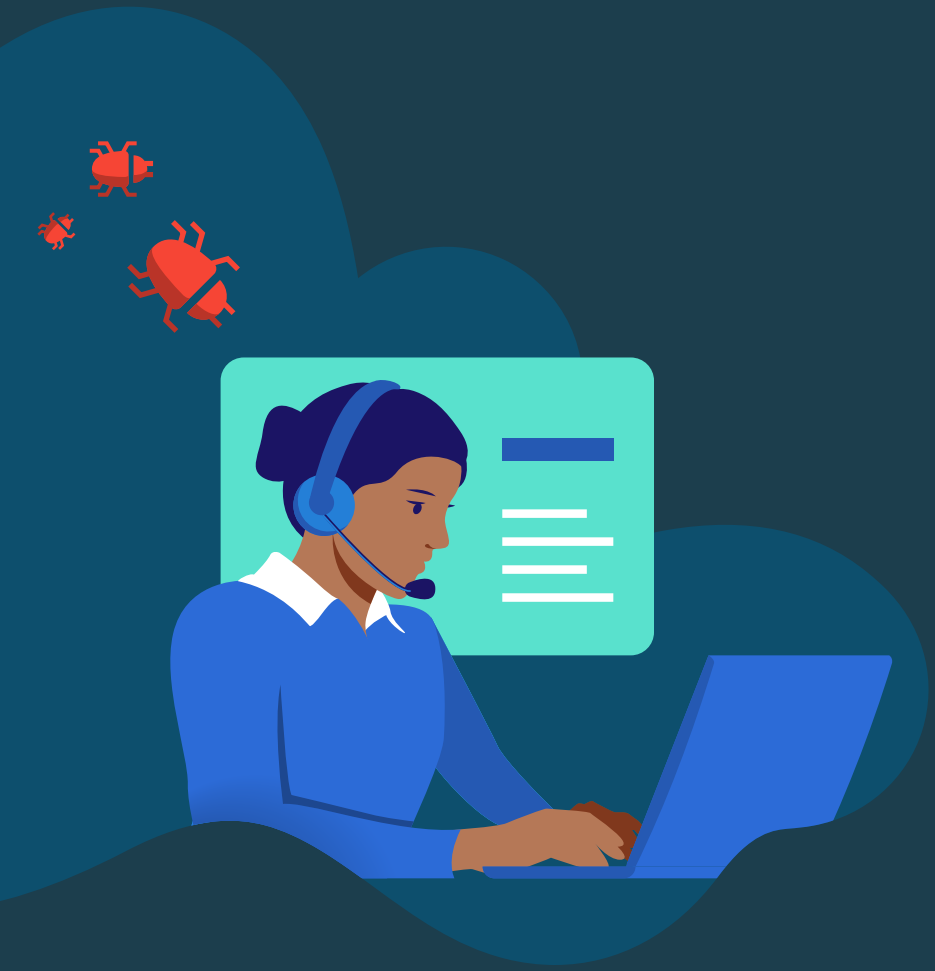
Dit jaar vroegen we MSP's welke sectoren het meest vatbaar waren voor aanvallen met ransomware door COVID-19. Het is niet verwonderlijk dat de gezondheidszorg bovenaan stond. 59% van MSP's zei dat ze dachten dat gezondheidszorg het meest kwetsbaar was. Hackers staan erom bekend een aanval in te zetten tegen slachtoffers die op de een of andere manier al zijn getroffen. Daarom is het logisch te denken dat cybercriminelen het op organisaties in de gezondheidszorg hebben gemunt tijdens de wereldwijde pandemie.

Financiën/verzekeringen was tweede (50%) en de overheid derde (45%). Het ligt voor de hand dat deze sectoren ook ernstig zijn aangetast door de pandemie. Buiten de top drie ziet de rest van de lijst er vrijwel hetzelfde uit als in vorige jaren.

De sectoren die vanwege COVID-19 het meest kwetsbaar waren voor ransomware:



*Respondenten konden uit meerdere antwoorden kiezen.



Hackers hebben het niet alleen op het MKB gemunt...

95% van de respondenten was het erover eens dat MSP's steeds meer het doelwit zijn van aanvallen met ransomware. Dit is waarschijnlijk te wijten aan een aantal hoogwaardige aanvallen op het MKB dat vers in het geheugen ligt. In aanvallen als deze gebruiken hackers MSP-referenties om toegang te verkrijgen tot hun klanten en ransomware te verspreiden. Met andere woorden, door een MSP in gevaar te brengen, krijgen cybercriminelen meer waar voor hun geld.

MSP's nemen de bedreiging serieus. Meer dan de helft maakt nu gebruik van tools voor wachtwoordbeheer en meervoudige verificatie, zoals u hieronder zult zien.

2FA- en SSO-gebruik

44% meldde dat ze een identiteitsprovider voor Single Sign-on (SSO) gebruiken. Microsoft Azure Active Directory was verreweg de eerste keuze voor SSO-identiteitsproviders onder respondenten. 47% van MSP's zei dat ze Azure AD voor SSO gebruiken. Daarvan gebruikt 44%, dus bijna 70% dezelfde provider voor tweevoudige verificatie (2FA).

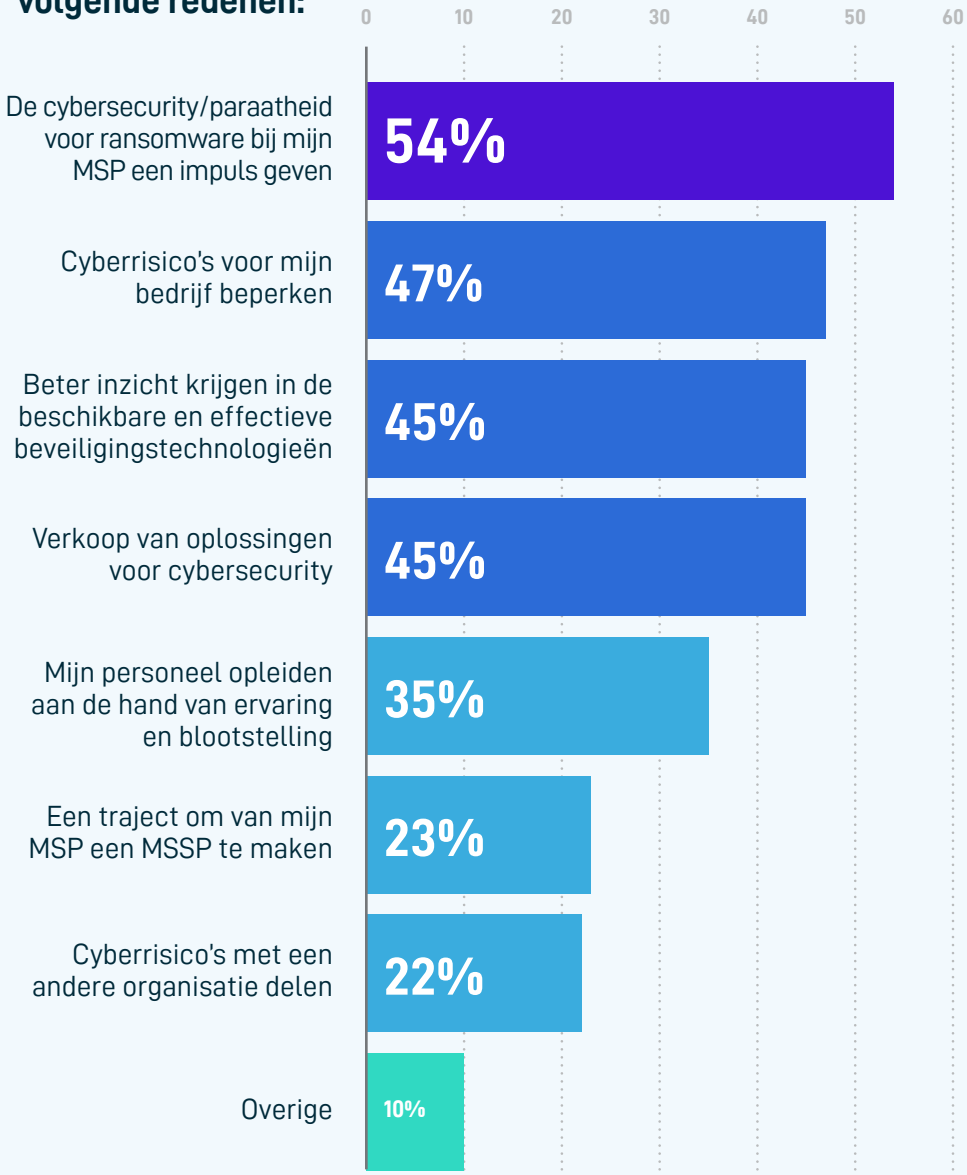
Bijna de helft van MSP's werkt samen met MSSP's

46% van MSP's werkt nu samen met managed security service providers (MSSP's) voor hulp met IT-beveiliging—voor hun klanten en hun eigen bedrijven. De belangrijkste reden die MSP's hiervoor meldden was om hun eigen beveiligingsparaatheid te verbeteren—nog een teken dat MSP's de mogelijkheid van aanvallen op hun eigen bedrijven serieus nemen.

Uiteindelijk komt de samenwerking met een MSSP neer op toegang tot deskundige bijstand. IT-beveiliging is een brede, complexe discipline waarvoor een specialisatie nodig is om expertise te ontwikkelen. MSSP's hebben deze expertise en MSP's hebben hem nodig.

46% van MSP's werkt nu samen met MSSP's voor hulp bij IT-beveiliging

MSP's die samenwerken met MSSP's noemden de volgende redenen:



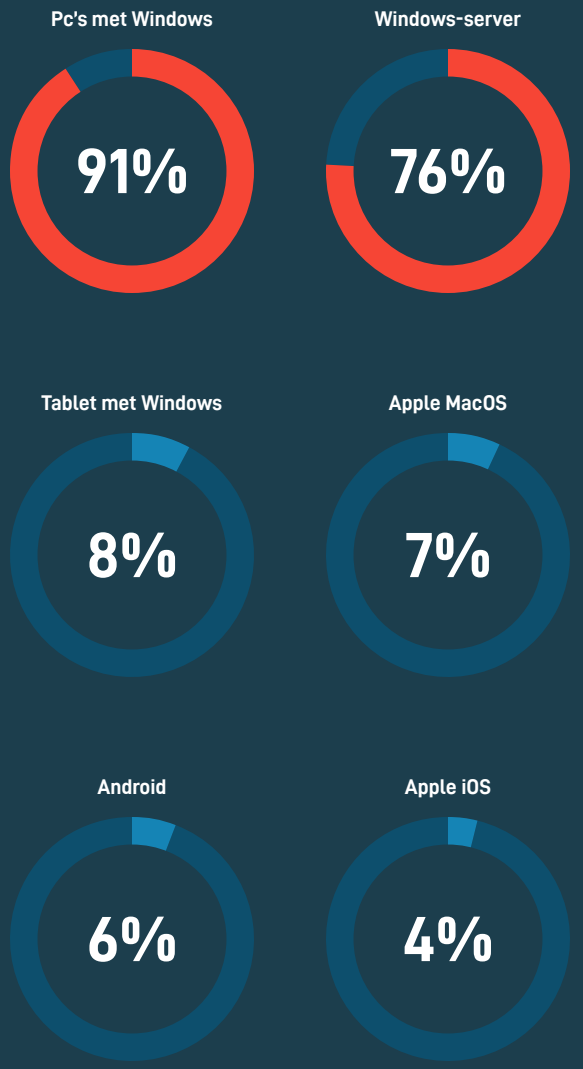
**Respondenten konden uit meerdere antwoorden kiezen.*

Windows Endpoint-systeemtoepassingen het belangrijkste doelwit van hackers

91% van ransomware had het volgens MSP's gemunt op pc's met Windows. Dit komt overeen met het feit dat phishing-e-mails de eerste aanvalsvector is en het grote aantal pc's met Windows dat vandaag de dag in gebruik is. Het benadrukt ook de noodzaak voor eindpuntbeveiliging en back-upoplossingen. Aanvallen met ransomware op deze systemen hebben een belangrijke impact op de productiviteit van gebruikers en op zijn beurt op de mogelijkheid van een bedrijf om opbrengsten te genereren. Oplossingen waarmee werknemers snel terug aan het werk kunnen na aanvallen moeten als essentieel worden gezien.

Windows-servers volgden met 76%. Dat is omdat ransomware een netwerk binnen kan komen via een phishing-e-mail. Zoals hiervoor vermeld, duurt het niet lang totdat de malware zich over het netwerk verspreidt en andere systemen besmet. Een oplossing voor bedrijfscontinuïteit die lokaal of in de cloud serverwerkbelastingen kan herstellen is van kritiek belang om bedrijfsonderbrekingen tot een minimum te beperken na een aanval met ransomware.

Eindpuntsystemen die het vaakst slachtoffer zijn van aanvallen met ransomware:



**Respondenten konden uit meerdere antwoorden kiezen.*

Ransomware kruipt SaaS-apps binnen

Bijna 1 op de 4 MSP's deed melding van aanvallen met ransomware op SaaS-toepassingen van klanten. Daarvan werd Microsoft het hardst getroffen. Dat is niet echt een verrassing omdat zo veel organisaties op Microsoft 365 vertrouwen. Het was wel enigszins verrassend dat meer dan de helft ransomware in Dropbox had. Google Workspace maakt de top drie compleet met 25%.

64%
van MSP's meldt aanvallen in Microsoft 365

54%
van MSP's meldt aanvallen in Dropbox

25%
van MSP's meldt aanvallen in Google Workspace

Menselijke fouten gebeuren: Hoe het back-uppen van SaaS kan helpen LEZEN

**Respondenten konden uit meerdere antwoorden kiezen.*

Meest gebruikte herstelmethodes tegen ransomware

Een nieuwe installatie op een machine vanaf een back-up was de belangrijkste herstelmethode tegen ransomware dit jaar. Dat is een belangrijke verandering ten opzichte van vorig jaar toen opnieuw installeren vanaf fabrieksinstellingen bovenaan stond. Dit jaar nam dat de derde plaats in ex aequo met het virtualiseren van het systeem vanaf een back-upkopie.

76%
Een machine vanaf een back-up herstellen

33%
Nieuwe installatie vanaf fabrieksinstellingen

27%
Software uitvoeren om een bedreiging te verwijderen

36%
Herstellen vanaf bestanden

31%
Het systeem virtualiseren vanaf een back-upkopie

15%
Betaalden losgeld

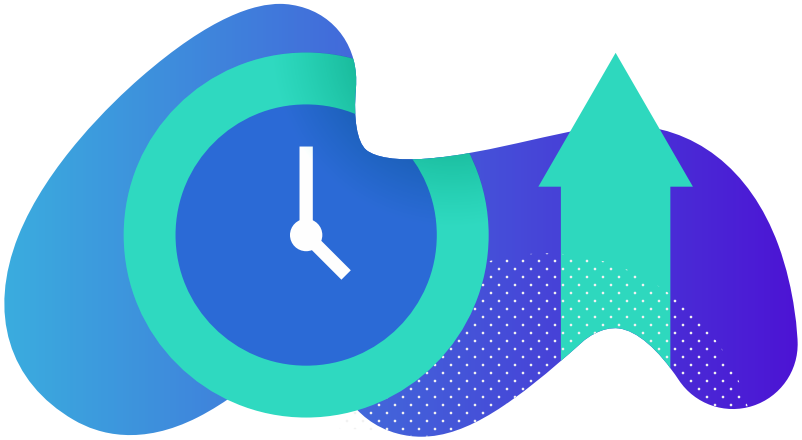
**Respondenten konden uit meerdere antwoorden kiezen.*

Ik ben blij dat 'opnieuw installeren vanaf een back-up' de eerste methode was die MSP's gebruiken om zich van aanvallen met ransomware te herstellen. Dit laat zien dat MSP's volwassener omgaan met hun herstelmethodes. Twee jaar geleden probeerden MSP's de shock van ransomware het hoofd te bieden door iets bij elkaar te scharrelen voor een herstel en installaties op machines helemaal opnieuw te doen. Vorig jaar was er al sprake van een verandering in aanpak door de juiste oplossingen aan te dragen bij hun klanten en uitvaltijd en gegevensverlies zoveel mogelijk te beperken. Nu beginnen we de resultaten te zien van die inspanningen, die tot uitdrukking komen in meer volwassen herstelmechanismen.

Ryan Weeks
Chief Information Security Officer, Datto, Inc.

BCDR-klanten lopen minder kans op aanzienlijke uitvaltijd

van MSP's zei dat klanten met BCDR-producten minder kans lopen op aanzienlijke uitvaltijd door ransomware.



Meest effectieve oplossingen om ransomware te bestrijden

- Bedrijfscontinuïteit en herstel na noodgevallen (BCDR)
- Training van werknemers
- Platform voor eindpuntdetectie en reactie
- Patch management
- Unified threat management
- Beheeroplossing voor identiteitstoegang
- Antivirus-/Antimalwaresoftware
- E-mail-/spamfilters
- Platform voor eindpunt-/mobiel beheer
- Browserisolatie

Wij eisen voor al onze klanten minimaal Datto SIRIS als een van de beveiligings-/continuïteitslagen die wij bieden. Voor mij is het net zo belangrijk als cybersecurity-verzekering. Wanneer we het met potentiële klanten over BCDR hebben, bespreken we de detectie en het herstel na ransomware. Maar we vertellen ook hoe snel we klanten op lokale failover laten werken. Onlangs had een lokaal politiebureau dat wij ondersteunen een serverstoring en wij konden ze in een kwestie van minuten met Datto SIRIS weer aan het werk zetten.

Brian J. Weiss
CEO, ITECH Solutions

Slotconclusies

1 **Het lijkt erop of het bewustzijn over ransomware toeneemt.** In het algemeen zijn er aanwijzingen dat MSP's en het MKB maatregelen treffen om aanvallen met ransomware te bestrijden. En hun inspanningen maken een impact. Hoewel het nog steeds om de meest voorkomende vorm van aanvallen met malware gaat, namen de aanvallen met ransomware vorig jaar iets af. Hogere beveiligingsuitgaven van het MKB, MSP's die samenwerken met MSSP's en het gebruik van beveiligingsmaatregelen zoals SSO en 2FA wijzen allemaal op een groter bewustzijn van beveiliging.

2 **Het MKB heeft meerdere oplossingen nodig om aanvallen te bestrijden.** De huidige ransomware heeft geen kind aan de standaard beveiligingsoplossingen van vandaag de dag. Organisaties kunnen worden binnengedrongen door phishing-aanvallen en de detectie door beveiligingsoplossingen vermijden. Om het risico op besmettingen te beperken is een meerlaagse benadering nodig, niet één enkel product.

3 **Het MKB moet de eerste verdedigingslinie voorbereiden: hun werknemers.** Bedrijven moeten vandaag de dag regelmatig en verplicht training op het gebied van cybersecurity krijgen zodat alle werknemers in staat zijn potentiële aanvallen te herkennen en vermijden. Hoewel de aanvallen dit jaar licht afnamen, zijn aanvallen met phishing nog steeds de meest succesvolle aanvalsvector, gevolgd door een aantal andere fouten van werknemers die met een betere beveiligingstraining zouden kunnen worden beperkt.

4 **Het MKB heeft behoefte aan een continuïteitsstrategie.** De gegevens van de enquête laten nogmaals zien dat er geen onfeilbare manier bestaat om aanvallen met ransomware te vermijden, ook niet met goede beveiligingsoplossingen. Daarom was bedrijfscontinuïteit dit jaar opnieuw de belangrijkste oplossing om deze aanvallen te bestrijden. Aangezien ransomware is bedacht om zich over netwerken en SaaS-toepassingen te verspreiden, zijn back-upoplossingen voor eindpunt en SaaS die zijn ontworpen voor een snel herstel van kritiek belang.

Aanvullende hulpmiddelen

Mogelijk bent u ook geïnteresseerd in:

Uitvaltijd van bedrijven beperken met een toolkit voor compleet herstel

Uitgebreide bescherming tegen ransomware: Detectie, reactie en herstel

RMM & Patch management: De eerste verdedigingslinie tegen cyberbedreigingen

Verhalen van mensen die ransomware hebben overleefd:

Datto en Interplay redden een klant van ransomware

Reading Buses blijven rijden dankzij Datto

Kennis is macht: Opleiding over ransomware voor werknemers:

Wat is ransomware?

Veelvoorkomende types ransomware

Veelvoorkomende aanvallen met phishing

5 soorten aanvallen met social engineering

9 tips over cybersecurity die MSP's hun klanten kunnen bieden

Voor een meerlaagse aanpak van ransomware:

Vraag een BCDR-demo van Datto aan

Vraag een Saas Protection-demo van Datto aan

Vraag een RMM-demo van Datto aan

Inschrijven op het Datto-blog

Bezoek de Datto-website

Al een partner van Datto?

Bekijk MarketNow voor de volledige eindgebruikercam-pagne over ransomware.

Over het rapport

Datto's rapport over de wereldwijde stand van zaken op het gebied van Channel Ransomware bestaat uit statistieken die uit een online enquête met meer dan 1.000 Datto-partners zijn gehaald, welke in de maand augustus van 2020 werd verspreid. Neem voor meer informatie over het rapport contact op met Katie Thornton, directeur Content- en Marketingsprogramma's bij Datto, Inc.

Over Datto

Als 's werelds toonaangevende leverancier van cloudgebaseerde software- en technologieoplossingen, geleverd door Managed Service Providers (MSP's), heeft Datto de overtuiging dat er geen grenzen zijn aan wat kleine en middelgrote bedrijven kunnen bereiken met de juiste technologie. 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

Volg ons op: Twitter, Instagram, Facebook, LinkedIn, YouTube
Schrijf u in voor ons blog: www.datto.com/blog
Schrijf u in voor onze podcast: www.datto.com/podcast