Rapport

datto

Het Global State of the Channel
Ransomware-rapport

Volg ons op:

Lees onze blogs op: **www.datto.com/blog**

Over dit rapport

Het Global State of the Channel Ransomware-rapport van Datto bevat de uitkomsten van een onderzoek onder meer dan 1.400 Managed Service Providers (MSP's), partners en klanten van Datto. Het rapport biedt uniek inzicht in de actuele situatie rond ransomware vanuit het perspectief van het IT-kanaal en hun mkb-klanten, die dagelijks met malware-infecties te maken hebben. Het rapport bevat een schat aan informatie over ransomware, waaronder trends van de afgelopen jaren, frequentie, doelen, impact en aanbevelingen voor het waarborgen van herstel en continuïteit nu de dreigingen blijven toenemen. Neem voor meer informatie over het rapport contact op met Katie Thornton, Director of Content & Marketing Programs bij Datto, Inc.

About Datto

Als 's werelds toonaangevende leverancier van IT-oplossingen geleverd door managed service providers (MSP's) gelooft Datto dat er geen limiet zit aan wat kleine en middelgrote bedrijven kunnen bereiken met de juiste technologie. Datto biedt business continuity en disaster recovery, netwerken, businessmanagement en back-up- en synchronisatieoplossingen en heeft daarnaast een uniek ecosysteem van partners gecreëerd. Dit ecosysteem levert Datto-oplossingen aan bedrijven overal ter wereld. Sinds zijn oprichting in 2007 heeft Datto honderden awards in ontvangst mogen nemen voor zijn snelle groei, uitstekende producten, superieure technische support en voor het bevorderen van een fijne werkplek. Het internationale hoofdkantoor van Datto staat in Norwalk, Connecticut (VS). Ook heeft het bedrijf vestigingen in Australië, Canada, China, Denemarken, Duitsland, Nederland, Singapore en het Verenigd Koninkrijk. Bezoek datto.com voor meer informatie.

De belangrijkste uitkomsten

- **Ransomware blijft de grootste cyberbedreiging.** In 2019 rapporteerde 85% van de MSP's ransomware als de meest voorkomende malwarebedreiging voor het mkb.
- **Alleen al in de eerste helft van 2019 rapporteerde 56% van de MSP's aanvallen tegen klanten.** 15% van de MSP's rapporteerde verschillende ransomware-aanvallen op één dag.
- **Gemiddeld zegt een op de vijf mkb-ondernemingen slachtoffer te zijn geweest van een ransomware-aanval.** Mkb'ers die hun IT niet hebben uitbesteed, lopen meer risico.*
- **Wanneer het gaat om ransomware-dreiging is er een kloof tussen MSP's en het mkb.** 89% van de MSP's is 'zeer bezorgd' over deze dreigingen, terwijl maar 28% van de mkb'ers dat gevoel heeft.
- **MSP's noemen phishing-e-mails als de belangrijkste oorzaak van een succesvolle aanval.** Een gebrek aan cybersecurity-training, zwakke wachtwoorden en slecht gedrag van gebruikers zijn andere belangrijke oorzaken.

- **De gevolgen van een ransomware-aanval kunnen desastreus zijn.** Bijna de helft van de MSP's geeft aan dat getroffen klanten downtime hebben ondervonden die hun bedrijfsvoering in gevaar bracht.
- **Het gemiddelde bedrag dat een hacker aan losgeld vraagt stijgt.** MSP's rapporteren een gemiddeld bedrag van ongeveer $5.900. Dat is een stijging van 37% ten opzichte van vorig jaar.
- **De kosten van downtime stegen met 200% procent per jaar** en zijn gemiddeld 23x hoger dan het losgeld dat werd geëist in 2019.
- **92% van de MSP's rapporteert dat klanten die gebruikmaken van BCDR-oplossingen (business continuity en disaster recovery) veel minder kans lopen op significante downtime tijdens een ransomware-aanval.** Vier op de vijf MSP's geven aan dat klanten die een BCDR-oplossing hebben binnen 24 uur of minder konden herstellen van een ransomware-aanval.
- **Mkb'ers zijn niet de enige bedrijven die het doelwit zijn van hackers.** Vier op de vijf MSP's zeggen ook zelf het doelwit te zijn van ransomware-aanvallen.

**Bron: Eigen onderzoek van Strategy Analytics met focus op de Noord-Amerikaanse mkb-markt.*

Verschillende typen malware gericht op het mkb

Welke van de volgende typen malware heeft uw klanten de afgelopen twee jaar getroffen?

61% van de MSP's geeft aan dat het mkb werd **getroffen door virussen**

54% van de MSP's geeft aan dat het mkb werd **getroffen door adware**

46% van de MSP's geeft aan dat het mkb werd **getroffen door spyware**

29% van de MSP's geeft aan dat het mkb werd **getroffen door cryptojacking**

26% van de MSP's geeft aan dat het mkb werd **getroffen door een remote access trojan**

20% van de MSP's zegt dat het mkb werd getroffen door rootkits
18% van de MSP's zegt dat het mkb werd getroffen door wormen
14% van de MSP's zegt dat het mkb werd getroffen door keyloggers
13% van de MSP's zegt dat het mkb werd getroffen door exploit kits

** De respondenten konden meerdere antwoorden selecteren.*

Ransomware is de nummer één-bedreiging voor het mkb

Van alle malware-dreigingen die impact hebben op het mkb is **ransomware de grootste bedreiging.**

85% van de MSP's rapporteert **aanvallen op mkb-bedrijven** in de afgelopen twee jaar

Alleen al in de eerste helft van 2019 zegt **56%** van de MSP's **aanvallen tegen klanten te hebben gezien**

15% van de MSP's **meldt meerde ransomware-aanvallen op dezelfde dag**

Geotrend:
In Australië en Nieuw-Zeeland rapporteert 91% van de MSP's aanvallen tegen mkb-bedrijven in de afgelopen twee jaar. Dat is wereldwijd het hoogste percentage.

1 op de 5

mkb-bedrijven zegt het **slachtoffer te zijn geweest van een ransomware-aanval.***

Mkb'ers die hun IT niet hebben uitbesteed krijgen gemiddeld vaker te maken met aanvallen.

** Bron: Eigen onderzoek van Strategy Analytics met focus op de Noord-Amerikaanse mkb-markt.*

Bewustwording rond ransomware: het mkb versus de MSP's

In 2019 zegt

28%

van de MSP's dat **mkb-bedrijven 'zeer bezorgd'** zijn over ransomware

Er is een kloof tussen het mkb en MSP's over de betekenis van een ransomware-dreiging

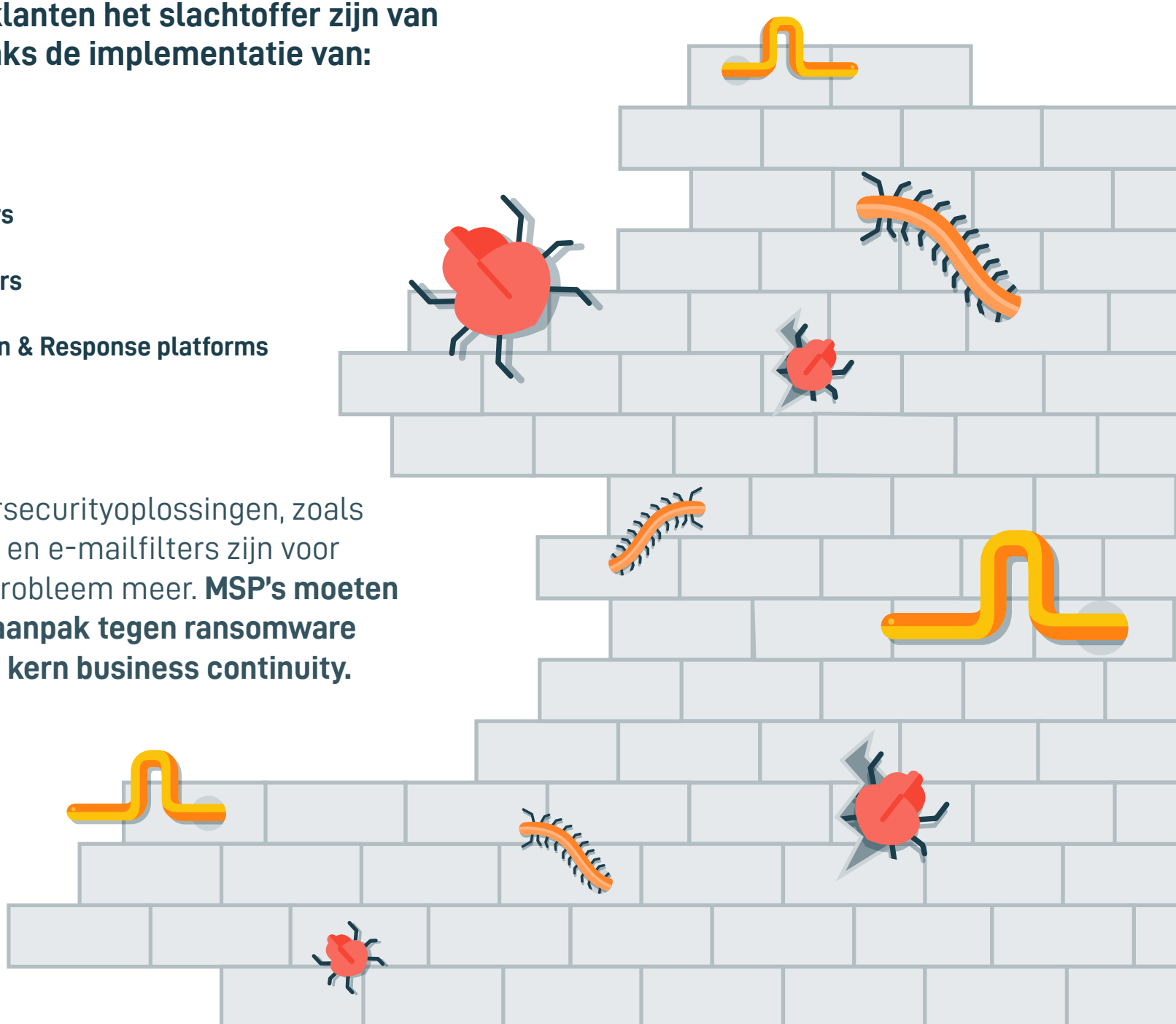
89%

van de MSP's zegt dat het **mkb 'zeer bezorgd'** zou moeten zijn over ransomware-dreiging

MSP's zeggen dat klanten het slachtoffer zijn van ransomware ondanks de implementatie van:

- **Antivirussoftware**
- **E-mail-/spamfilters**
- **Ad-/pop-up blockers**
- **Eindpointprotection & Response platforms**

Traditionele cybersecurityoplossingen, zoals antivirussoftware en e-mailfilters zijn voor aanvallers geen probleem meer. **MSP's moeten een meerlaagse aanpak tegen ransomware hanteren, met als kern business continuity.**



Wat zijn de belangrijkste oorzaken van ransomware?

67% van de MSP's rapporteert
phishing-e-mails

36% van de MSP's rapporteert
een gebrek aan cybersecurity-training

30% van de MSP's rapporteert
zwakke wachtwoorden/zwak access management

25% van de MSP's rapporteert slecht gedrag van de gebruiker
16% van de MSP's rapporteert kwaadaardige websites/web-advertenties
16% van de MSP's rapporteert clickbait

Phishing, gebrek aan cybersecurity-training en zwakke wachtwoorden zijn de drie meest genoemde oorzaken van een succesvolle ransomware-aanval.

** De respondenten konden meerdere antwoorden selecteren.*

Ransomware-aanvallen: de consequenties

Welke van de volgende consequenties waren het gevolg van een ransomware-aanval?

64% van de MSP's rapporteerde
verlies van productiviteit

45% van de MSP's rapporteerde
downtime van bedrijfsvoering

34% van de MSP's rapporteerde
het verlies van data

33% van de MSP's rapporteerde
een infectie aan een ander apparaat binnen het netwerk

29% van de MSP's rapporteerde
een afnamen van winstgevendheid bij hun klanten

24% van de MSP's rapporteerde
dat klanten losgeld betaalden om hun data terug te krijgen

18% van de MSP's rapporteerde reputatieschade
12% van de MSP's rapporteerde gestolen data
10% van de MSP's rapporteerde dat ransomware op systemen bleef staan en opnieuw toesloeg
7% van de MSP's rapporteerde dat ze niet in staat waren om compliant te zijn
6% van de MSP's rapporteerde dat ze niet konden voldoen aan SLA's
4% van de of MSP's rapporteerde dat klanten losgeld betaalden maar de data niet terugkregen

Bereken de kosten van potentiële downtime met onze Recoverytime- en Kostencalculator

BEREKEN

** De respondenten konden meerdere antwoorden selecteren.*

De kosten van downtime schieten omhoog

Bij een ransomware-aanval zijn de kosten van downtime volgens MSP's

23X hoger dan het geëiste losgeld

Gemiddeld losgeld

2018 $4,300 → **2019** $5,900

MSP's rapporteerde dat het gemiddelde bedrag aan losgeld met 37% is toegenomen ten opzichte van vorig jaar

Gemiddelde kosten downtime

2018 $46,800 → **2019** $141,000

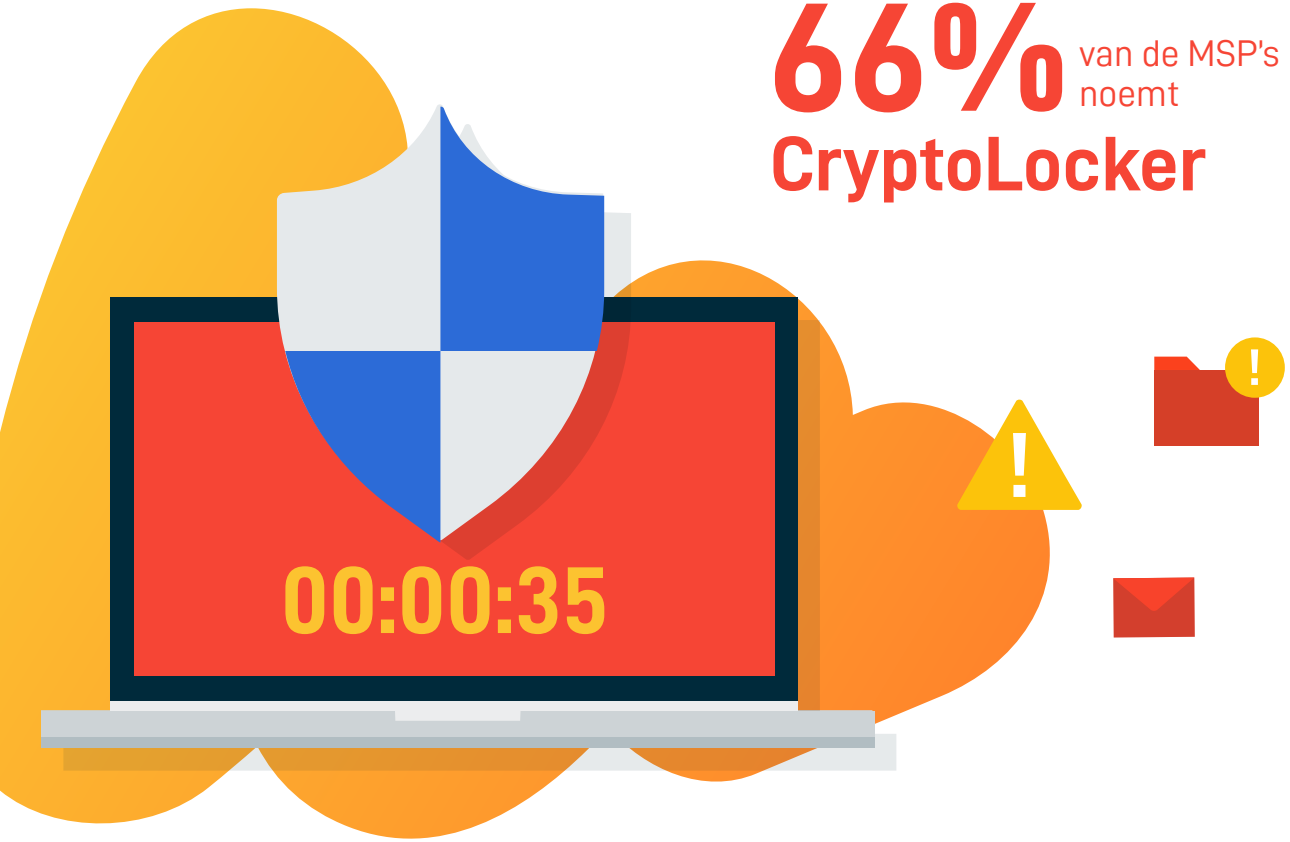
De gemiddelde kosten van downtime stegen met ongeveer 200% ten opzichte van vorig jaar

Geotrend:

In Canada rapporteerden de MSP's de hoogste gemiddelde kosten voor downtime: $180,000.

**Alle respondenten hebben de vragen beantwoord in U.S. dollars.*

Met welke van de volgende varianten van ransomware hebben uw klanten te maken gehad?



66% van de MSP's noemt
CryptoLocker

49% van de MSP's noemt
WannaCry

34% van de MSP's noemt
CryptoWall

24% van de MSP's noemt
Locky

17% van de MSP's noemt Petya
14% van de MSP's noemt CryptXXX
12% van de MSP's noemt notPetya
11% van de MSP's noemt TeslaCrypt
10% van de MSP's noemt Emotet **(nieuw)**
7% van de MSP's noemt CBT Locker
7% van de MSP's noemt TorrentLocker
7% van de MSP's noemt CrySis
6% van de MSP's noemt Bad Rabbit
5% van de MSP's noemt Wallet **(nieuw)**
4% van de MSP's noemt CoinVault

MSP's rapporteren voor het vierde opeenvolgende jaar **CryptoLocker als de belangrijkste malware-variant** die klanten aanviel.

** De respondenten konden meerdere antwoorden selecteren.*

Sectoren die vaak slachtoffer zijn van ransomware

32% an de MSP's rapporteert

dat de bouw- en de productiesector het meest door ransomware worden aangevallen.

Het is niet opmerkelijk dat de bouw- en de productiesector belangrijke doelwitten zijn. Deze branches bewegen mee met de schommelingen in de economie. Hierdoor wordt er relatief vaak projectmatig gewerkt en is terugkerende omzet een uitzondering. Dit zorgt ervoor dat er relatief weinig wordt geïnvesteerd in IT-medewerkers of IT-diensten die op maandelijkse basis worden afgenomen.

Vince Tinnirello, Managing Director, Anchor Network Solutions

31% Professional Services
23% Gezondheidszorg
20% Finance/verzekeringen
18% Non-Profit
18% Juridisch
15% Retail
12% Vastgoed
9% Architectuur/design
9% Overheid
8% Onderwijs
7% Consumentenproducten
5% Reiswereld/transport
6% Media/entertainment
4% High-tech
4% Energie/nutsbedrijven
2% Telecom
11% Overige/geen

** De respondenten konden meerdere antwoorden selecteren.*

Windows-werkplekken worden het meest aangevallen door hackers

89% van de MSP's rapporteert

ransomware die werkplekken aanviel

Van deze 89% rapporteert...

87% van de MSP's aanvallen op **Windows-pc's**

11% van de MSP's rapporteert aanvallen op Windows Tablet
7% van de MSP's rapporteert aanvallen op MacOS X
5% van de MSP's rapporteert aanvallen op Android
3% van de MSP's rapporteert aanvallen op iOS

Geotrend:

In Europa rapporteert 10% van de MSP's dat ransomware Android-systemen infecteert; **dat is 5% meer dan het wereldwijde gemiddelde.**

** De respondenten konden meerdere antwoorden selecteren.*

Ransomware richt zich op Office 365

28% van de MSP's rapporteert **ransomware-aanvallen op SaaS-applicaties**

Van deze 28% rapporteert:

64% van de MSP's aanvallen binnen Office 365

(een stijging van 49% ten opzichte van 2018)

47% van de MSP's aanvallen in Dropbox

18% van de MSP's aanvallen in G Suite

6% van de MSP's aanvallen in Box
2% van de MSP's aanvallen in Salesforce

Mkb-bedrijven zeggen dat tussen de 11% en 50% van hun IT-infrastructuur in de cloud is ondergebracht. De meeste bedrijven verwachten over 3 jaar dat tussen de 21% en 75% in de cloud zal draaien.**

Geotrend:

In **Australië en Nieuw-Zeeland rapporteert 37%** van de MSP's aanvallen op SaaS-applicaties, het hoogste **percentage wereldwijd.**

** De respondenten konden meerdere antwoorden selecteren.*
*** Bron: Eigen onderzoek van Strategy Analytics met focus op de Noord-Amerikaanse mkb-markt.*

Welke methoden heeft u gebruikt om uw klant te helpen data te herstellen na een ransomware-infectie?

69% van de MSP's noemt het

re-imagen van een apparaat

53% van de MSP's noemt het

virtualiseren van het systeem door een back-up-image

37% van de MSP's noemt het

draaien van software om de dreigingen weg te nemen

16% van de MSP's noemt een specifieke softwaretool die is ontwikkeld om te herstellen na een ransomware-aanval

15% van de MSP's vertrouwt op eind-punt-antivirus voor herstel

12% van de MSP's noemt als oplossing het vinden van een decryptie-sleutel

Hoe rapid rollback MSP's helpt klanten te herstellen van ransomware

** De respondenten konden meerdere antwoorden selecteren.*

Het kan lastig zijn om de bron van een ransomware-dreiging te identificeren of hoelang de dreiging al aanwezig is in een bepaalde omgeving. Daardoor vermoeden we dat MSP's verschillende methoden gebruiken om te herstellen, waarbij ze de situatie van geval tot geval bekijken. **MSP's hebben herstelplannen nodig die inspelen op de tactieken van alle bedreigingen waar hun klanten mee te maken hebben.** Zij kunnen daarvoor verschillende vendoren kiezen die herstelopties bieden die op maat gemaakt kunnen worden. Afhankelijk van het betreffende incident moeten zij een plan opstellen om er zeker van te zijn dat de back-ups veilig zijn, zelfs na een dreiging die mogelijk lange tijd op de achtergrond heeft gesluimerd.

Ryan Weeks, Chief Information Security Officer, Datto

BCDR wordt door MSP's als de nummer één-oplossing aanbevolen.

- Business Continuity and Disaster Recovery (BCDR)
- Trainen van medewerkers
- Patch management
- Unified threat management
- Identity and access management
- Antivirus- en malwaresoftware
- E-mail- en spamfilters
- Endpoint & Mobile Management Platforms
- Browser-isolatie
- Endpointdetection en respons-platforms (nieuw)

Traditionele antivirusoplossingen zijn alleen effectief voor het detecteren van dreigingen die al bekend zijn. Ransomware is inmiddels instaat deze detectie-engines te omzeilen. Endpointdetection en -respons software kijkt hoe een proces samenwerkt met het besturingssysteem en meldt of blokkeert activiteiten die lijken op malware.

David Thomas, Group Managing Director, Bluegrass Group Ltd

Met BCDR is herstel na een ransomware-aanval 4x waarschijnlijker

92% van de MSP's

zegt dat klanten die gebruikmaken van BCDR-oplossingen minder kans hebben op significante downtime door ransomware

4 op de 5 MSP's zeggen dat klanten met BCDR volledig hersteld zijn binnen 24 uur of minder

Without BCDR,

Minder **dan 1 op de 5** was daartoe in staat zonder BCDR

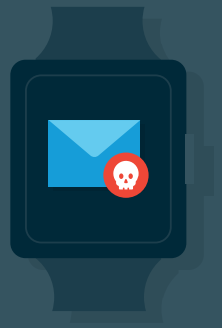
Vraag een Datto BCDR demo aan

Lees hier meer

96% van de MSP's

voorspelt dat de aanvallen doorgaan en mogelijk verergeren

IoT staat boven aan de lijst van ransomware-aanvalsdoelen



64% van de MSP's voorspelt dat ransomware **IoT-devices zal aanvallen**

Waarom IoT?

Veel van deze apparaten zijn niet ontworpen met security in het achterhoofd. Cybercriminelen zullen manieren vinden om deze kwetsbaarheid te benutten. Er zijn in 2020 naar verwachting meer dan 20 miljard IoT-devices, die hackers meer toegangspunten in netwerken bieden.

Dale Shulmistra, CEO, Invenio IT

63% van de MSP's voorspelt dat ransomware **social media-accounts zal aanvallen**

56% van de MSP's voorspelt dat ransomware **kritische infrastructuren gaat infecteren (bijvoorbeeld het stroomnet)**

62% van de MSP's voorspelt dat een bedrijf failliet kan gaan door een ransomware-aanval

49% van de MSP's voorspelt dat ransomware **zich gaat richten op gebruikers op basis van demografische kenmerken**

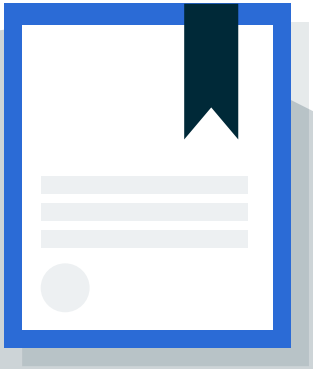
4 op de 5

MSP's zijn het erover eens dat hun eigen bedrijf steeds vaker het doelwit is van ransomware-aanvallen.

De beste aanpak is een goede verdediging:

60% van de MSP's heeft een **verzekering voor cyberaansprakelijkheid, mochten** zij of hun klanten het slachtoffer worden van een ransomware-aanval

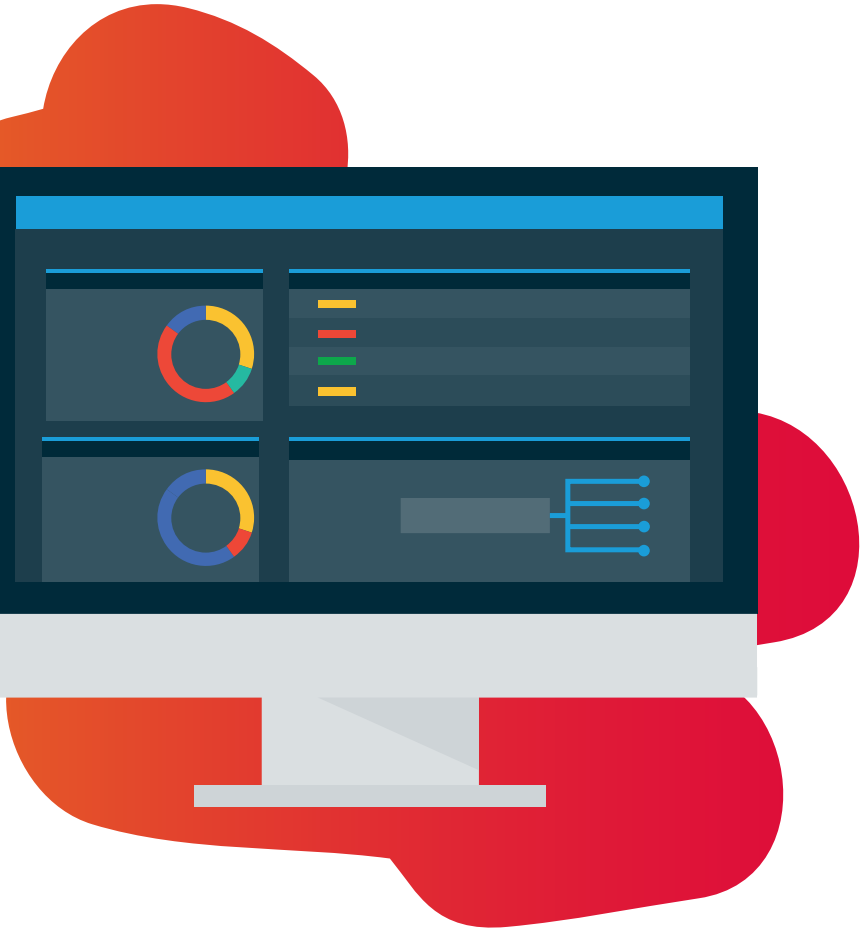
50% van de MSP's heeft **externe expertise klaar staan om te helpen** als er sprake is van een grootschalige aanval tegen hun systemen of die van hun klanten



MSP's die een aansprakelijkheidsverzekering voor cyberaanvallen overwegen, **moeten starten met het checken van hun eigen verzekeraar waar ze al een aansprakelijkheidsverzekering** hebben om te bepalen wat de dekking is.

In deze turbulente tijden moeten MSP's het voortouw nemen. Zij moeten zichzelf beschermen om hun klanten veilig te houden. MSP's moeten tweefactor-authenticatie invoeren voor elke technologie die zij en hun klanten gebruiken. In een klimaat waar cyber-aanvallen dagelijks voorkomen, **is tweefactor-authenticatie voor alle technologieoplossingen een van de meest effectieve manieren om de kansen op een succesvolle aanval te verminderen.**

Ryan Weeks, Chief Information Security Officer, Datto



MSP's melden dat ze tweefactor-authenticatie (2FA) gebruiken voor de volgende tools en applicaties:

71% Remote Monitoring and Management (RMM)

61% Wachtwoord-manager

56% IT-documentatie

60% Email Client

43% BCDR

58% Professional Services Automation (PSA)

In het nieuws: **Nieuwe dreigingen onderstrepen belang tweefactor-authenticatie**

Vraag een Datto RMM demo aan

Lees hier meer

De belangrijkste conclusies:

Bedrijven moeten de eerste laag van hun bescherming voorbereiden: de medewerkers. Bedrijven moeten vandaag de dag regelmatig verplichte cybersecurity-trainingen bieden om ervoor te zorgen dat alle werknemers potentiële phishing-e-mails in hun inbox herkennen. Phishing is immers een belangrijke ingang voor ransomware.

Bedrijven moeten verder meerdere oplossingen gebruiken om zich voor te bereiden op het ergste. De standaard beveiligingsoplossingen zijn niet opgewassen tegen de huidige ransomware, die organisaties op meerdere manieren kan binnendringen. Het verminderen van het risico op infecties vereist een meerlaagse aanpak in plaats van één enkel product.

Bedrijven hebben een continuïteitsstrategie nodig. Er is niet één bewezen manier om ransomware te voorkomen, hoewel antivirussoftware, perimeterbeveiliging en patchbeheer essentieel zijn. Bedrijven moeten zich concentreren op manieren om de bedrijfsvoering te handhaven na een ransomware-aanval. Een solide, snelle en betrouwbare BCDR-oplossing is onderdeel van die strategie. Omdat er ook ransomware is die via netwerken en SaaS-applicaties verspreid worden, zijn endpoint en SaaS backup-oplossingen voor snel herstel van groot belang.

Bedrijven hebben een apart aanspreekpunt voor cyberbeveiliging nodig om de bedrijfscontinuïteit te waarborgen. Mkb-bedrijven vertrouwen vaak op iemand die het erbij doet en het leuk vindt om IT-ondersteuning te bieden. Maar als een bedrijf zich geen eigen IT-medewerker kan veroorloven voor 24/7/365 cybersecurity-monitoring, dan is het slim om gebruik te maken van een managed service provider (MSP) die de tijd en middelen heeft om te anticiperen op dreigingen en een bedrijf kan beschermen tegen de nieuwste cybersecurity-bedreigingen.

Meer informatie:

Misschien vindt u dit ook interessant:

Kennis is macht

Ransomware – training voor medewerkers:

- Wat is Ransomware?
- Veel voorkomende typen ransomware om in de gaten te houden
- 5 vormen van social engineering

Ransomware – verhalen van over-levenden:

- Datto en Interplay behoeden een klant voor Ransomware
- masterIT houdt vliegtraining in de lucht tijdens ransomware annval
- Cole Informatics verzekert Vick Insurance van doorang bij Ransomware ramp

Voor een meerlaagse benadering van ransomware:

- Vraag een Datto BCDR demo aan
- Vraag een Datto SaaS Protection demo aan
- Vraag een Datto RMM demo aan

- Abonneer u op de Datto-blog
- Ga naar de website van Datto

Bent u al een Datto-partner?

Kijk dan op MarketNow voor de complete eindgebruikerscampagne over ransomware.