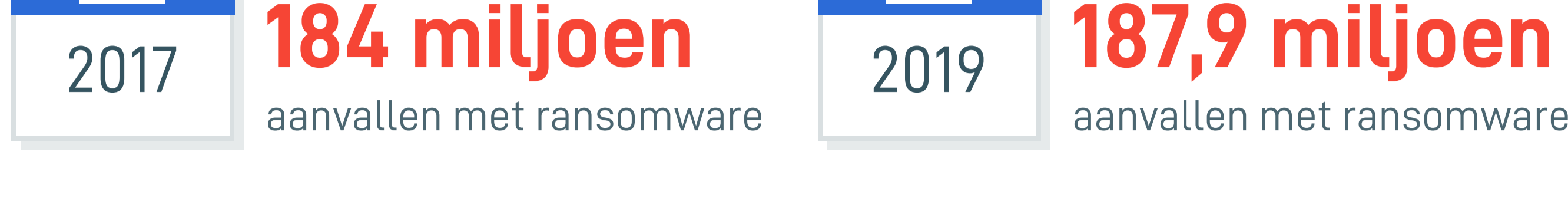


Ransomware en de kosten voor uitvaltijd

Tegen 2021 zal een bedrijf elke 11 seconden slachtoffer worden van een aanval met ransomware.

De toename van ransomware



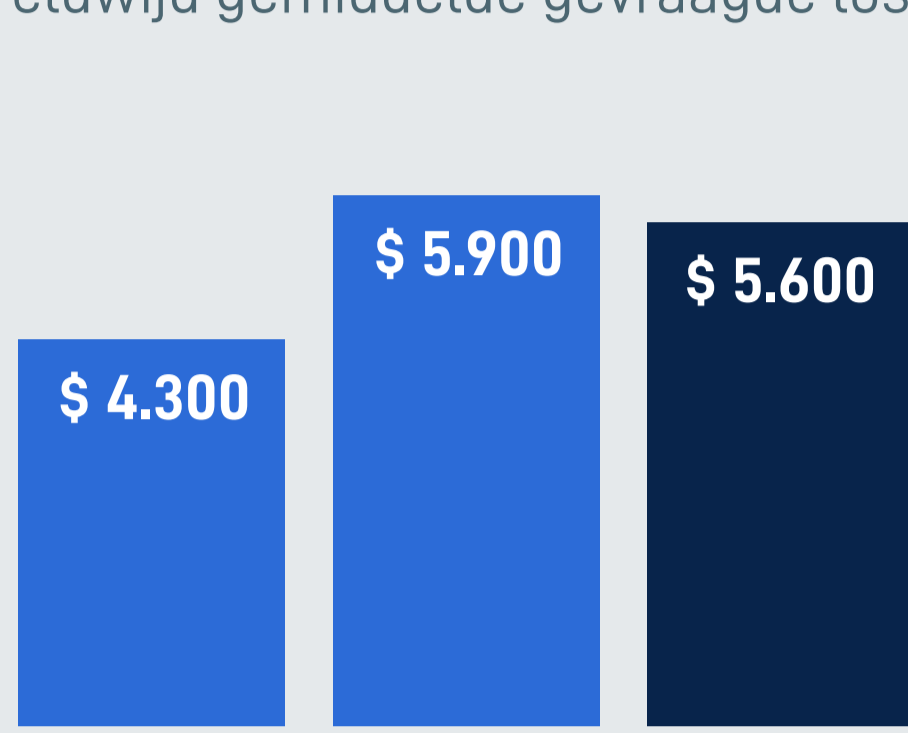
In de eerste helft van 2020 namen aanvallen met ransomware met 715% toe omdat cybercriminelen de COVID-19-pandemie gingen uitbuiten



Ongeveer de helft van bedrijven over heel de wereld wordt elk jaar door ransomware getroffen

Aanvallen met ransomware brengen 2,5 keer zoveel schade toe dan ander incidenten met cybersecurity

Wereldwijd gemiddelde gevraagde losgeld



Gemiddelde kosten van uitvaltijd ten gevolge van een aanval



Aanvallen worden steeds geavanceerder

Aanvallers hebben het gemunt op back-upoplossingen die ze versleutelen om de kans te vergroten dat het slachtoffer het losgeld zal betalen

Nieuwe ransomware maakt gebruik van Wake-on-LAN om meer netwerkapparatuur aan te zetten en zijn verspreiding te vergroten

Hackers hebben het gemunt op managed service providers (MSP's) om met één enkele aanval toegang te krijgen tot meerder bedrijven

Uitvaltijd na een aanval kan bijna 50 keer meer kosten dan het losgeld zelf

De ware kosten van uitvaltijd

Na een aanval zijn bedrijven waardevolle tijd kwijt om hun systemen te herstellen



Netwerken repareren



Back-ups herstellen



Verloren apparaten vervangen

Door ransomware veroorzaakte uitvaltijd is met \$ 274.200 een kostbare zaak

Betalen of niet betalen - Beide betekenen uitvaltijd

98%

van de bedrijven die losgeld betalen, ontvangt van de hackers een programma voor ontsluiting

Dat betekent dat ze nog steeds met kostbare uitvaltijd te maken hebben wanneer ze hun gegevens ontsleutelen – 4% slaagt er nooit in de versleutelde gegevens terug te krijgen

34%

van bedrijven heeft meer dan een week nodig om van ransomware te herstellen

Voor sommigen kan een volledig herstel maanden duren



91% van MSP's zegt dat

klanten met een bedrijfscontinuïteit en een plan voor herstel na noodgevallen (BCDR) minder kans lopen op aanzienlijke uitvaltijd ten gevolge van ransomware

Bedrijfscontinuïteit en herstel na noodgevallen (BCDR)

Waarom BCDR?

Uitgebreide BCDR zal:

- Tijdens een beveiligingsincident of noodgeval de uitvaltijd beperken
- Belangrijke informatie snel herstellen zodat onderbrekingen minimaal zijn
- Helpen bij de naleving van de voorschriften
- U laten zien welke lessen er na een incident kunnen worden geleerd

4 op de 5 kleine ondernemingen

met BCDR herstellen zich binnen 24 uur van ransomware

Belangrijke functies voor maximale veerkracht



Snelle failback

Maakt gebruik van een "Rescue Agent" voor herstel na noodgevallen en voert een continu gespiegelde bare metal recovery uit



Detectie van ransomware

Geautomatiseerde scans naar ransomware na back-ups en gegevens- en bootverificatie zorgen ervoor dat u het zo snel mogelijk weet als een aanval met ransomware is gedetecteerd



Snel terugdraaien

Maakt een naare een back-up omkering mogelijk naar een eerdere status zonder opnieuw te hoeven formatteren of partitioneren



Tweevoudige verificatie

Zorgt voor een back-up oplossing om te voorkomen dat aanvallen met ransomware gegevens in gevaar brengen



Directe virtualisatie

Beperkt uitvaltijd na een aanval of uitval met behulp van virtualisatie in de cloud of lokaal



Veilige back-up in de cloud

Een offsite, veilige, SOC 2-conforme cloudinfrastructuur via georeplicatie maakt een noodgeval mogelijk



Datto's Cloud Deletion Defense

Maakt gegevensherstel over de risicovectoren heen mogelijk - zelfs wanneer de beschermde machine is gecompromitteerd.

Datto biedt een helpende hand in de strijd om uw klanten tegen ransomware te beschermen.

Bezoek vandaag www.datto.com/products/continuity.

Bronnen

- datto.com/products/siris
- comparitech.com/antivirus/ransomware-statistics
- Datto's rapport over de stand van zaken op het gebied van ransomware - 2019 & 2020
- cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
- statista.com/statistics/701282/ransomware-experience-of-companies
- statista.com/statistics/494947/ransomware-attacks-per-year-worldwide
- csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
- cdn.securelist.com/files/2017/11/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf
- datto.com/resource-downloads/Datto2019_StateOfTheChannel_RansomwareReport.pdf
- blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019
- coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
- arrow.com/ecs/na/channeladvisor/channel-advisor-articles/what-is-bcdr-and-why-is-it-important
- blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis
- mystateline.com/news/local-news/winnipeg-county-it-experts-talk-cyber-security-amid-rps-breach
- bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
- info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf
- propublica.org/article/the-new-target-that-enables-ransomware-hackers-to-paralyze-dozens-of-towns-and-businesses-at-once

datto

DEVELOPED BY
NEWSOURCING