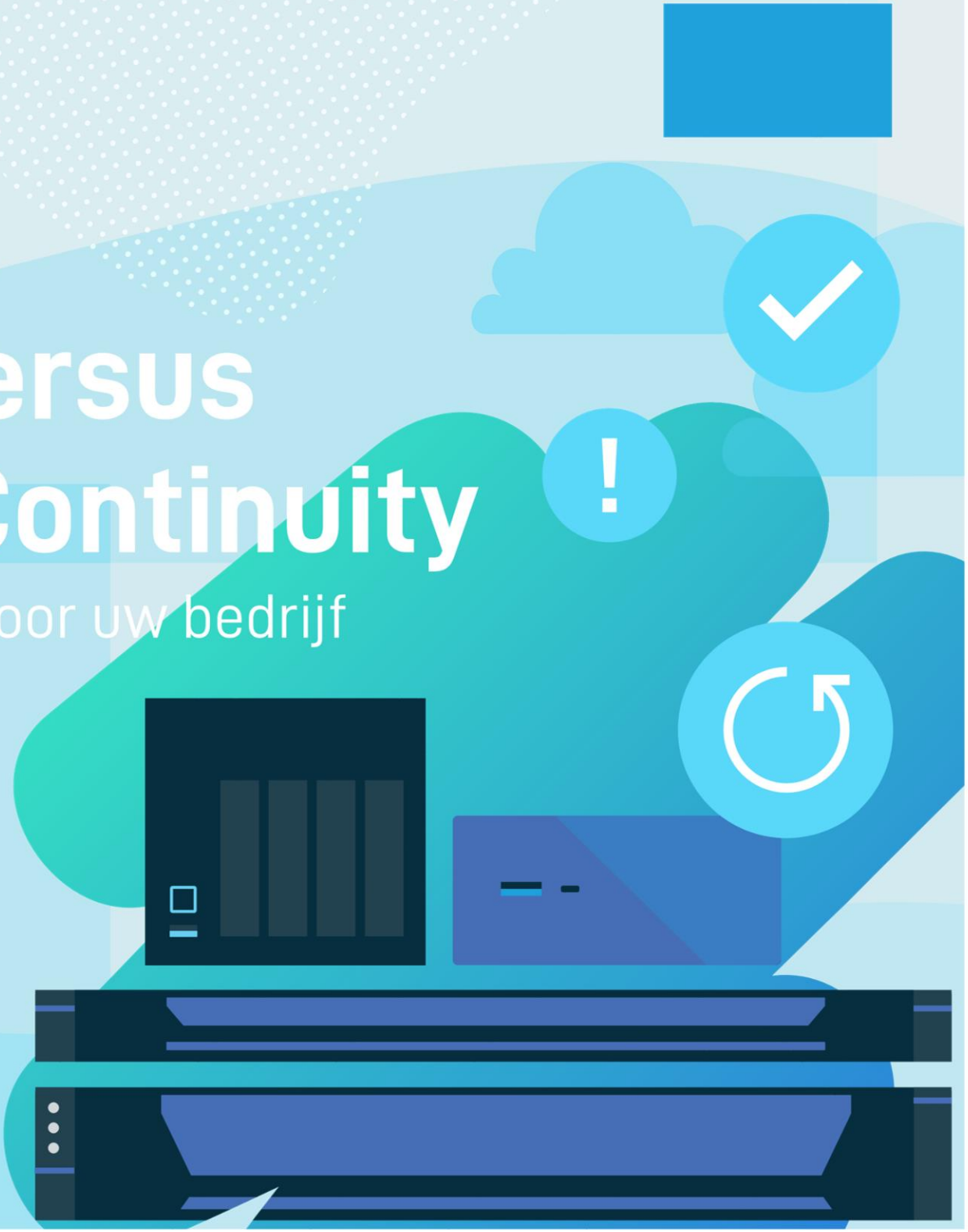
eBook

Back-up Versus Business Continuity

Een betere planning voor uw bedrijf



Dataprotectie-oplossingen zijn essentieel voor ieder bedrijf, ongeacht de omvang, de industrie waarin het actief is of de locatie ervan. In dit whitepaper bespreken we waarom business continuity meer is dan het simpelweg maken van back-ups. Daarnaast zetten we uiteen hoe je interne herstelprocessen en downtimekosten kunt evalueren, zodat jij de beste oplossing vindt voor jouw behoeften.

Introductie

Downtime is kostbaar. Hoe kostbaar? Dat is volledig afhankelijk van de omvang van een organisatie, maar per uur liggen die kosten gemiddeld tussen de 8.000 en 80.000 euro. Het gemiddelde Britse bedrijf ligt 27 uur per jaar plat (dat is langer dan de rest van Europa) en dat kost de Britse economie meer dan 2,2 miljard euro per jaar. De getallen liegen er niet om.

Wat veroorzaakt downtime? Netwerkstoringen en menselijke fouten veroorzaken respectievelijk 50 procent en 45 procent van de downtime. Verder wordt tien procent van de downtime veroorzaakt door natuurrampen. Maar ook ransomware zorgt de laatste jaren steeds vaker voor downtime. Hierbij worden de data van een bedrijf gegijzeld totdat er losgeld is betaald.

Wanneer we kijken naar de oorzaak van downtime op basis van datavolume, is de grootste boosdoener menselijke fouten, met 58 procent. Dit wijst erop dat bedrijven beter op hun eigen medewerkers moeten letten, en zich minder zorgen hoeven te maken over natuurrampen. Stel jij dataprotectie steeds uit omdat jouw organisatie zich niet in de buurt bevindt van een uiterwaard? Wees dan gewaarschuwd: de grootste dreiging voor jouw data bevindt zich binnen de muren van jouw bedrijf, niet erbuiten.

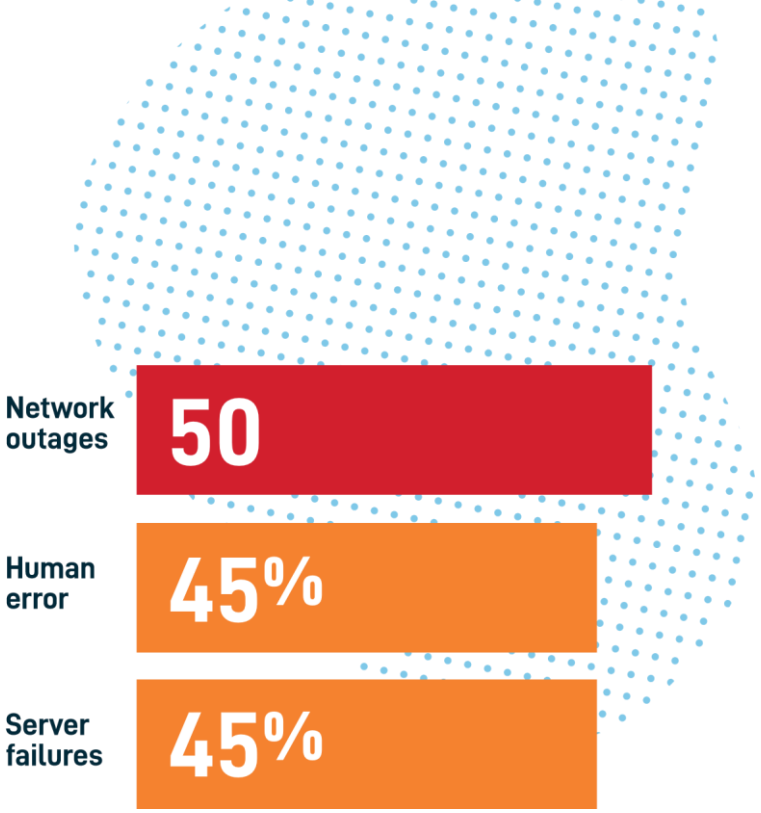


Figure 1: Reasons for downtime

Wat staat er op het spel?

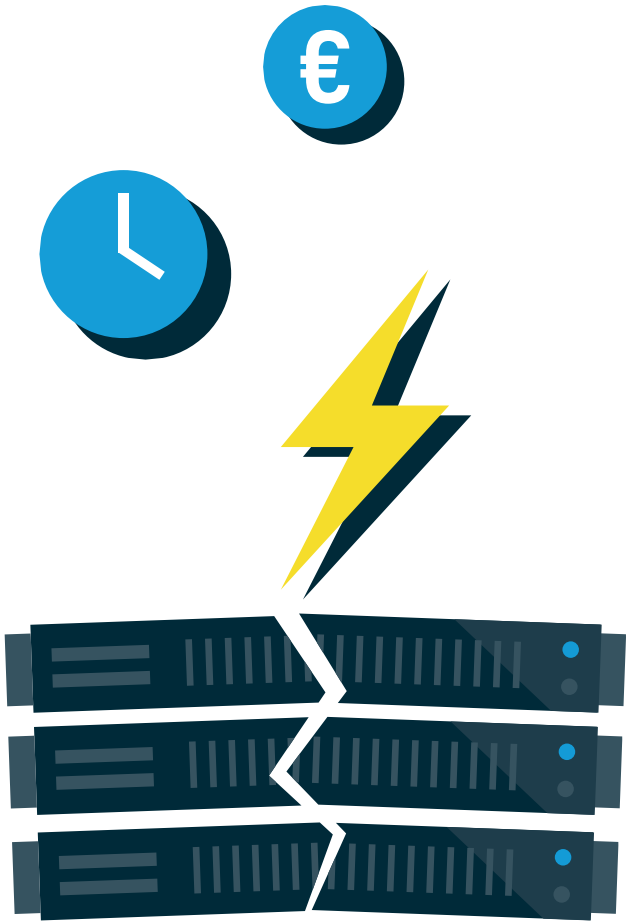
Dagelijks wordt er 2,5 quintiljoen bytes aan data gegenereerd. En 90 procent van de nu bestaande data is de afgelopen jaren gecreëerd, waarvan een significant deel door kleine bedrijven. Gezien de hoeveelheid servers, desktops en laptops die door veel mkb-bedrijven wordt beheerd, moet er dus heel veel data worden beschermd.

Toch heeft bijna 75 procent van de mkb-bedrijven geen distaster recoveryplan en is slechts 25 procent ‘heel zeker’ dat ze de mogelijkheid heeft om data te herstellen. 50 procent van de mkb-bedrijven maakt een back-up van minder dan 60 procent van hun data. En de overige 40 procent? Die wordt helemaal niet beschermd.

Hoeveel die downtime bedrijven kost? De afgelopen jaren verloor 35 procent van de mkb-bedrijven meer dan 340.000 euro vanwege downtime. En een heel ongelukkige 3 procent raakte hieraan meer dan 750.000 euro kwijt. Alleen al ransomware kostte Britse bedrijven in 2016 meer dan 5 miljoen euro – en de 25 procent die losgeld betaalde kreeg hierna niet de data terug.

Wanneer een bedrijf wordt getroffen door downtime, probeert het allereerst zo snel mogelijk belangrijke data terug te halen. Volgens IDG duurt het zo’n 7 uur voordat een bedrijf na een incident met dataverlies weer volledig functioneert. 18 procent van de IT-managers geeft aan dat het 11 tot 24 uur duurt, of zelfs langer.

De afgelopen jaren verloor 35 procent van de mkb bedrijven meer dan 340.000 euro vanwege downtime.



De Aberdeen Group trok dezelfde conclusie toen het best-in-class bedrijven vergeleek met gemiddeld presterende bedrijven en achterblijvers op het gebied van downtime en herstel. En zelfs als je de gemiddelde tijd, die het kost om data te herstellen (5,18 uur) vermenigvuldigt met de gemiddelde kosten die downtime met zich meebrengt, is het resultaat een flink hoge rekening. Deze rekening bestaat voornamelijk uit verloren manuren, verminderde productiviteit, herstelkosten, verloren klanten (bestaande of potentiële), reputatieschade, en afgeleide of gefrustreerde medewerkers en andere aandeelhouders.

Wat doen mkb-bedrijven om zichzelf te beschermen? Meer dan 60 procent slaat nog fysiek tapes op in een opslaglocatie of een andere vestiging. En dat is een verrassend hoog percentage, want de technologie is al vier decennia oud en de opslag- en herstelprocessen zijn zeer omslachtig. 20 procent van de mkbbedrijven gebruikt echter wel al een vorm van cloud databack-up.

Lokale of cloud back-up? Het antwoord ligt ertussenin

Als het op snel herstel en business continuity aankomt, werkt lokale back-up het best. Met name omdat de gegevens binnen handbereik zijn en snel een eenvoudig terug te zetten zijn naar hun originele locatie. Zo blijft het bedrijf actief. Maar wat gebeurt er als de stroom uitvalt? Als het apparaat ermee stopt? Of wordt gestolen of vernietigd in bijvoorbeeld een natuurramp? Hierdoor lijkt de cloud misschien aantrekkelijker. Maar alleen cloud back-up brengt ook risico's met zich mee, omdat je niet altijd controle hebt over de vereiste bandbreedte om jouw gegevens goed te back-uppen. Daarnaast zijn de herstelprocessen vaak complex en tijdrovend. En ook de cloud werkt weleens niet.

Meer dan 90 procent van het mkb gaat binnen twee jaar failliet na getroffen te zijn door een ramp.

Veel bedrijven wenden zich daarom tot een hybride-cloudoplossing. Hierbij wordt eerst jouw data gekopieerd en opgeslagen op een lokaal apparaat. Zo kan je als er iets gebeurt snel een eenvoudig vanaf dat apparaat herstellen. Maar jouw data worden ook in de cloud opgeslagen. Als er dan iets gebeurt met het apparaat, beschik je over aparte kopieën van jouw data – zonder dat je de data fysiek hebt moeten verplaatsen.

Databack-up versus business continuity: wat is het verschil?

Databack-up beantwoordt de vragen: zijn mijn data veilig? Kan ik ze terughalen in het geval van een storing? Business continuity draait meer om het bedrijf in het algemeen en stelt daarbij de vraag: hoe snel krijg ik mijn bedrijf weer up and running in het geval van een systeemuitval?

Het overwegen van databack-up is een goede eerste stap. Maar business continuity is net zo belangrijk, omdat het ervoor zorgt dat jouw bedrijf binnen afzienbare tijd weer naar behoren functioneert wanneer het noodlot toeslaat. Als jouw server bijvoorbeeld zou ophouden met werken, zou je met slechts een back-up op bestandsniveau niet weer aan het werk kunnen. Jouw server zou vervangen moeten worden, software en data opnieuw geïnstalleerd en het hele systeem zou opnieuw moeten worden aangepast op basis van jouw instellingen en voorkeuren. Dit proces kan dagen in beslag nemen. Kan jouw bedrijf zich die tijd wel veroorloven?

Wanneer het over business continuity gaat, hebben we het over Recovery Time Objective (RTO) en Recovery Point Objective (RPO).

RTO: de Recovery Time Objective is de tijdsduur waarin een bedrijf hersteld moet zijn na een storing, zodat onacceptabele consequenties worden voorkomen.

RPO: de Recovery Point Objective is de maximaal toegestane periode waarin data verloren mogen zijn naar aanleiding van een storing.

Door jouw gewenste RTO te berekenen, bepaal je de maximale tijd waarin jij zonder data mag zitten voordat jouw bedrijf risico loopt. Een andere optie is om de RPO vast te stellen, zodat jij weet hoe vaak er een back-up gemaakt moet worden. Misschien heb je een RTO van een dag, of een RPO van een uur – dat is volledig afhankelijk van de behoeften van jouw bedrijf. Met deze twee doelstellingen kan jij bepalen welke oplossing voor databack-up je nodig hebt (zie afbeelding 6).

Nadat je jouw RPO en RTO hebt vastgesteld, is het tijd om te berekenen hoeveel downtime en verloren data je eventueel kunnen kosten. Tel per uur de gemiddelde salariskosten, overheadkosten en inkomsten bij elkaar op en je weet precies hoeveel dataverlies je kost.

Ook kan je gebruikmaken van deze gratis eenvoudige online RTO-calculator voor direct inzicht in RPO, RTO en downtimekosten.

Aangezien budgetbeperkingen een uitdaging zijn voor veel bedrijven, kunnen deze hoge kosten een goede reden zijn voor het aanschaffen en onderhouden van een business continuity-oplossing.

Lokale of cloudback-up? Het antwoord ligt er tussenin. Een hybride cloud-oplossing maakt gebruik van zowel de voordelen van lokaal backups als van de veiligheid van de cloud.

De berekening van de daadwerkelijke kosten van dataverlies geeft je de financiële validatie die je nodig heeft om een business continuity oplossing te rechtvaardigen.

Image versus file-only back-up

Er bestaan twee bekende soorten back-upoplossingen: file- en image-based. Een file-based back-up doet precies wat je denkt: je kiest welke bestanden je wilt back-uppen, en die bestanden worden opgeslagen op een lokaal apparaat of in de cloud, ongeacht het type oplossing dat je heeft gekozen. Maar alleen de geselecteerde bestanden zijn opgeslagen. Wat als je een belangrijk bestand vergeet? Image-based back-up slaat een image op van jouw data in de bijbehorende omgeving. Dit houdt in dat je exacte kopieën hebt van wat er op de server staat opgeslagen – inclusief het besturingssysteem, instellingen en voorkeuren. Als een server plat komt te liggen, kan je deze binnen een paar minuten herstellen, in plaats van de uren of dagen die het duurt om een nieuwe server aan te schaffen, installeren en instellen.

Waar moet je op letten bij een business continuity-oplossing?

Hier volgt een aantal zaken waar je op moet letten als je op zoek gaat naar een geschikte business continuity-oplossing.

- Hybride-cloudback-up – Een hybride aanpak lost de kwetsbaarheden op die een cloud- of lokale oplossing met zich meebrengen.
- Goede RTO en RPO – Kijk niet alleen naar back-up, maar let ook op business continuity en bereken hoeveel downtime jouw bedrijf aankan (RTO) en hoeveel dataverlies jij je kunt veroorloven (RPO).
- Image-based back-up – Zorg ervoor dat de back-upoplossing een image opslaat van alle data en systemen, in plaats van bestanden handmatig te kopiëren.

Meer informatie nodig
over de mogelijkheden?
Kijk op onze website hier

Fastbyte Wiersedreef 10, 3433 ZX te Nieuwegein

www.Fastbyte.nl