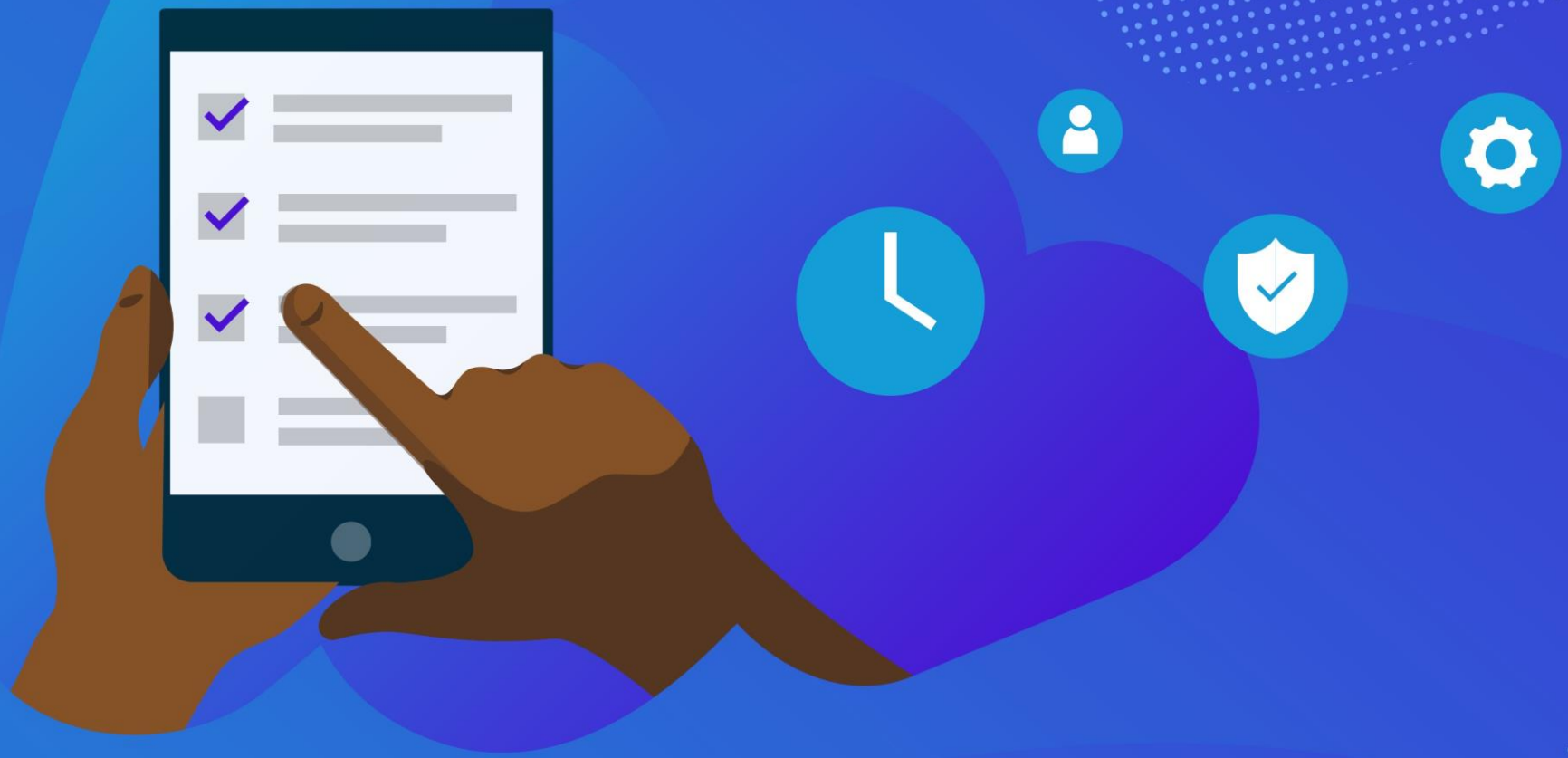
eBook



4 tips voor een bedrijfscontinuïteitsplan

Stel een doeltreffend bedrijfscontinuïteitsplan op door naar het totaalplaatje te kijken

Invoering

Het is mooi als jouw bedrijf belangrijke toepassingen gebruikt, maar als jouw kantoor onder water staat en jouw werknemers thuis zonder stroom zitten, kan je er weinig mee. Om na een incident aan de behoeften van jouw klanten te kunnen blijven voldoen moet je de onderneming van jouw klant als geheel bekijken.

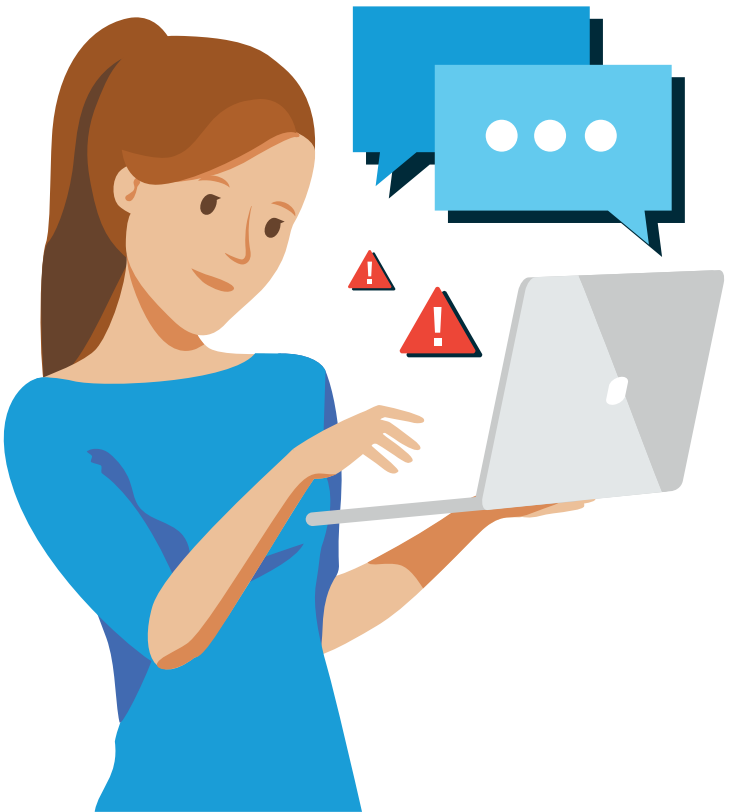
Bij veel bedrijven moet hiervoor in eerste instantie een bedrijfsimpactanalyse (BIA) worden uitgevoerd. In dit e-book gaan we hier niet uitgebreid op in, maar dit zijn de doelstellingen van een BIA:

- Potentiële gebeurtenissen identificeren die de normale bedrijfsactiviteiten negatief zouden kunnen beïnvloeden
- Van iedere gebeurtenis berekenen hoe waarschijnlijk het is dat deze optreedt
- Bepalen wat deze gebeurtenis voor gevolgen zou kunnen hebben voor jouw bedrijf

Als uw datacenter zich bijvoorbeeld vlak bij het water bevindt in een laaggelegen gebied, is een overstroming een potentiële gebeurtenis. Tijdens de winter is de kans op een overstroming groter. Als er sprake is van significante downtime, zou dit erg negatieve gevolgen kunnen hebben voor jouw bedrijf. Bedrijven kunnen te maken krijgen met veel verschillende bedreigingen, van natuurrampen tot beveiligingslekken tot willekeurige ongelukken. Een lekkende pijpleiding kan even grote gevolgen hebben als een overstroming, wanneer de pijpleiding zich precies boven een kritische server bevindt.

Nadat je deze stappen hebt gevolgd, kan je concrete plannen opstellen voor risicobeperking, rampenbestrijding en bedrijfscontinuïteit. In dit e-book geven we jou vier tips voor een bedrijfscontinuïteitsplan die allemaal met elkaar te maken hebben.

Het is erg belangrijk dat er een veiligheids- en communicatieplan voor jouw werknemers is dat werkt.



1. Besteed Zorg Aan Het Welzijn Van Jouw Werknemers

Er komen veel verschillende uitdagingen kijken bij de communicatie tijdens en na een noodgeval. Daarom is het erg belangrijk dat er een veiligheids- en communicatieplan voor jouw werknemers is dat werkt. De specifieke kenmerken van zo'n veiligheids- en communicatieplan voor noodgevallen verschillen per bedrijf, maar de volgende punten moeten in ieder geval in dit plan worden opgenomen:

• Hoe het bedrijf ervoor zorgt dat de werknemers veilig zijn tijdens een rampsituatie.

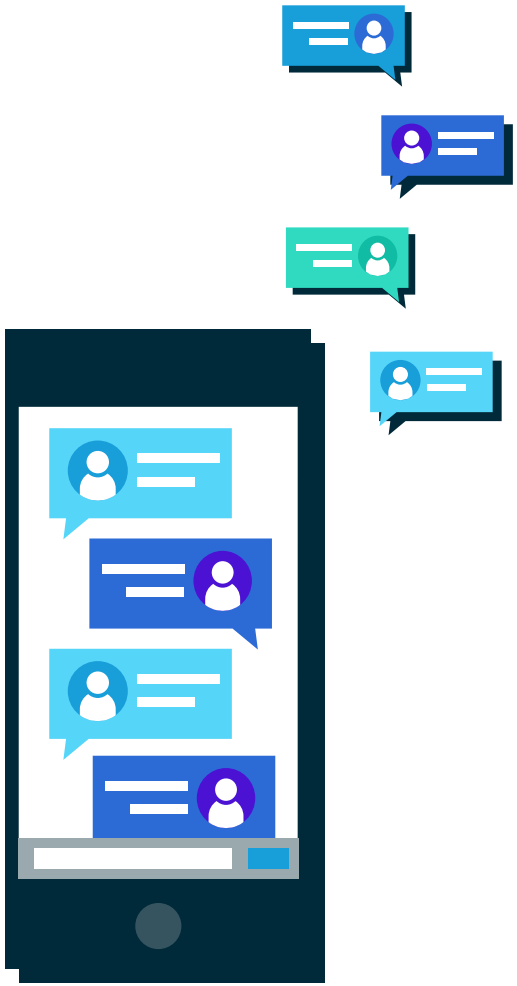
• Hoe het bedrijf na de gebeurtenis essentiële informatie communiceert aan de werknemers.

Het eerste punt is erg afhankelijk van de aard en locatie van jouw bedrijf. Zo zal het veiligheidsplan van een grote productiefaciliteit er natuurlijk heel anders uitzien dan dat van een klein makelaarskantoor. Hierdoor is het erg lastig om specifieke richtlijnen te geven voor dit gedeelte van jouw plan voor bedrijfscontinuïteit en hersteloperaties. Het is in ieder geval belangrijk dat je jouw veiligheidsplan afstemt op de specifieke behoeften van jouw organisatie.

Voor het tweede punt moet je eerst de informatie verzamelen en zorgen dat deze goed wordt gedocumenteerd, eenvoudig toegankelijk is en op meerdere veilige locaties wordt bewaard. Dit geldt bijvoorbeeld voor up-to-date contactgegevens van werknemers (e-mailadressen, mobiele en vaste telefoonnummers, contactgegevens voor noodgevallen, enz.). In de informatie moet ook een werkwijze staan om contact op te nemen met de werknemers.

Effectieve communicatie

E-mail is natuurlijk de makkelijkste manier om een grote groep werknemers te bereiken, maar dat wordt lastig als de e-mailserver van jouw bedrijf is uitgevallen.



Het beheren van de relatie met jouw klanten is natuurlijk essentieel voor het voortdurende succes van jouw bedrijf.

Sommige bedrijven maken gebruik van extra Exchange-servers of cloudservices om ervoor te zorgen dat de werknemers toegang hebben tot hun e-mail. Jij hebt natuurlijk wel een alternatief nodig als je helemaal geen internet toegang meer hebt.

Een telefoonboom, ook wel ‘belboom’, ‘bellijst’ of ‘telefoon keten’ genoemd, is een andere populaire methode om tijdens en na een gebeurtenis belangrijke informatie door te geven aan werknemers. Dat werkt als volgt: Een bepaalde werknemer start de telefoonboom door de volgende werknemer in de lijst te bellen. Die werknemer neemt vervolgens contact op met de volgende persoon in de lijst. Dat gaat zo door totdat iedereen in de lijst is gebeld. Andere bedrijven sturen automatische noodoproepen door middel van speciale communicatiesoftware/-services.

Wat voor methode je ook gebruikt om jouw werknemers te informeren, jouw communicatieplan voor noodgevallen moet voldoende gedetailleerd zijn om het ook uit te kunnen voeren als de maker van het plan na het noodgeval niet aanwezig is (bijvoorbeeld vanwege letsel of onbegaanbare wegen). Het plan moet ook flexibel genoeg zijn, zodat het in verschillende noodsituaties kan worden gebruikt. Zo zal de reactie op een brand in uw faciliteit tijdens werktijd veel verschillen van de communicatie na de grootschalige distributie van een defect product. De communicatie moet in noodsituaties kort en zo nauwkeurig mogelijk zijn. Afhankelijk van de structuur van jouw organisatie kan het zijn dat je jouw managers op de hoogte wilt houden, zodat zij de informatie kunnen doorgeven aan hun directe ondergeschikten voor zover dit nodig is. Ook in dit geval wordt de juiste aanpak bepaald door de kenmerken van jouw bedrijf.

Tot slot is het erg belangrijk om het communicatieplan periodiek te testen en aan te passen. Hierdoor kan je de gaten in het plan dichten, zoals verouderde werknemerslijsten of contactgegevens.

Het vermogen van jouw bedrijf om na een gebeurtenis antwoord te kunnen bieden op de behoeften van jouw klanten, is rechtstreeks van invloed op de reputatie van jouw bedrijf.

2. Houd Jouw Klanten Op De Hoogte

Het beheren van de relatie met jouw klanten is natuurlijk essentieel voor het voortdurende succes van jouw bedrijf. Daarom is het belangrijk om een plan op te stellen om jouw klanten te informeren tijdens en na een incident. De omvang van jouw klant-communicatieplan is sterk afhankelijk van de aard van jouw bedrijf.

Het is natuurlijk niet nodig om jouw klanten op de hoogte te brengen van ieder mankement. Als er echter een situatie optreedt die waarschijnlijk ook voor jouw klanten gevolgen heeft, is het belangrijk om hun de details van het probleem te vertellen en uit te leggen welke maatregelen je neemt om het probleem op te lossen. Het kan zijn dat je dan rechtstreeks contact moet opnemen met jouw klanten of dat je ze een bericht kunt sturen via traditionele en sociale media. Doe je dat niet, dan kan dit de reputatie van jouw organisatie beschadigen.

Neem bijvoorbeeld de manier waarop Toyota in 2009-2010 reageerde op meldingen van zelf-accelererende voertuigen. In plaats van het probleem te erkennen en de klanten gerust te stellen dat de situatie werd onderzocht, zei het bedrijf dat de gebruiker een fout had gemaakt: een klassiek voorbeeld van de schuld neerleggen bij het slachtoffer. Uiteindelijk gaf het bedrijf aan dat het probleem werd veroorzaakt door de vloermatten, het ontwerp van de gaspedalen en defecte elektronica. Hoewel ze bij Toyota miljarden uitgaven om onderdelen te vervangen, wekte de eerste reactie wantrouwen op bij hun klanten.

Na een incident moet je ook met een grote hoeveelheid binnenkomende communicatie kunnen omgaan. Afhankelijk van de aard van jouw bedrijf zijn dit bijvoorbeeld ondersteuningsverzoeken, een grote hoeveelheid e-mails en telefoontjes, berichten op sociale media van gefrustreerde klanten, media-aandacht, enzovoort. Het vermogen van jouw bedrijf om na een gebeurtenis antwoord te kunnen bieden op de behoeften van je klanten, is rechtstreeks van invloed op de reputatie van jouw bedrijf.

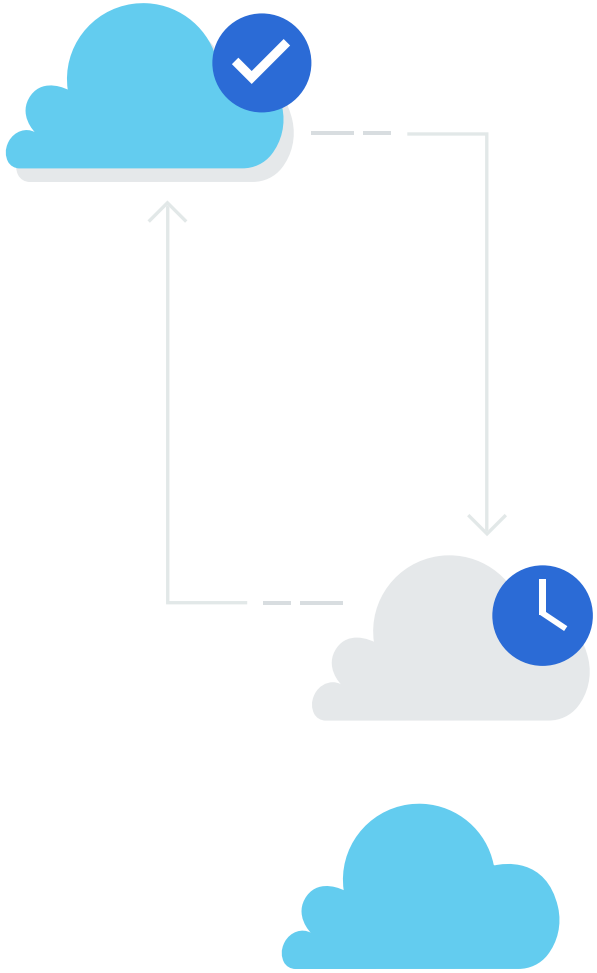
Je reputatie beschermen

Hoe kan je jouw goede reputatie intact houden? Het komt neer op een zorgvuldige voorbereiding. Ten eerste moet jouw personeel goed voorbereid zijn. Het is essentieel om de communicatie met klanten zorgvuldig te plannen. Je moet snel kunnen reageren en duidelijk kunnen uitleggen welke maatregelen je neemt om het probleem op te lossen.

Alle werknemers die rechtstreeks contact hebben met klanten, moeten worden geïnstrueerd en moeten een helder en consistent verhaal kunnen overbrengen. Je kunt hierbij gebruik maken van scripts die aan de situatie kunnen worden aangepast. De berichten kunnen van tevoren worden opgesteld, door het management worden goedgekeurd en vervolgens na een incident snel aan klanten worden verspreid.

Je moet ook ervoor zorgen dat er toegang is tot de communicatie-infrastructuur (telefoon, e-mail, internet). Hiervoor kan het zijn dat je extra telefoonlijnen/diensten, gehoste PBX-systemen of cloudbased e-mail- of Exchange-servers nodig hebt. Grotere bedrijven moeten mogelijk investeren in een secundair contactcentrum voor het inkomende en uitgaande communicatieverkeer. Er zijn verschillende leveranciers die voor callcenter diensten, tijdelijke werkplekken of zelfs mobiele datacenters kunnen zorgen.

Daarnaast is het ook belangrijk om het klant-communicatieplan geheel of gedeeltelijk te testen of te oefenen. Dit is de beste manier om de zwakke punten van de klantenondersteuning te identificeren en te verbeteren, maar ook om problemen met de communicatie-infrastructuur op te lossen.



Zorg dat er toegang is tot de communicatie-infrastructuur (telefoon, e-mail, internet)

3. Optimaliseer De Uptime Van Jouw IT-Systemen

Om de huidige rol van IT bij bedrijfscontinuïteit en hersteloperaties te begrijpen, moeten we naar het niet zo verre verleden kijken. Het is namelijk nog niet eens zo lang geleden dat een back-up bestond uit dagelijkse incrementele en wekelijkse volledige back-ups op tape of andere backup-media. Er werden reservetapes gemaakt die naar andere locaties werden verstuurd voor hersteloperaties. Dit was meestal een secundaire locatie die door het bedrijf zelf werd beheerd of een tapeopslaglocatie (zoals Iron Mountain). Tegenwoordig wordt dit model nog altijd door veel bedrijven gebruikt. Afhankelijk van jouw herstelbehoeften kan het ook een prima manier zijn.

Het kan echter bijzonder lang duren om data te herstellen met behulp van tapes die zich op een andere locatie bevinden. Eerst moeten de tapes worden opgehaald van die andere locatie. Vervolgens moeten de data worden overgebracht naar de back-upserver. Dan kan je eindelijk de data en toepassingen op jouw primaire servers herstellen. Dit leidt natuurlijk tot significante downtime.

Bij het maken van een IT-herstelplan moet je twee concepten duidelijk voor ogen hebben: Recovery Time Objective (RTO, beoogde hersteltijd) en Recovery Point Objective (RPO, beoogd herstelpunt). RTO is hoelang het duurt om een systeem na een defect of incident te herstellen. In het bovenstaande voorbeeld zou jouw RTO 48 uur of meer kunnen zijn. RPO is een eerder moment in de tijd waarnaar de data na een incident kunnen worden hersteld. Als je bijvoorbeeld elke dag om 18.00 een back-up maakt en de server de dag erna om 17.00 uitvalt, heb je een RPO van 23 uur. Je raakt dan alle data kwijt die in deze periode zijn gemaakt. Voor veel organisaties was dit onaanvaardbaar.

In plaats van tapes te gebruiken voor hersteloperaties, dupliceerden ze daarom de data van hun datacenter op een secundaire locatie.

Door recovery-in-place wordt de RTO significant verbeterd doordat de werknemers kunnen doorwerken terwijl de primaire servers worden hersteld.

Bij deze methode moest er echter veel geld worden geïnvesteerd in hardware, omdat de bedrijven twee sets identieke servers, opslaglocaties, switches, software, enz. nodig hadden, en dan hebben we het nog niet eens over het tweede datacenter. Door de data op afstand te dupliceren, kunnen de gebruikers bij een incident op de secundaire locatie verder werken. Hierdoor wordt de RTO verminderd, maar financieel gezien is deze optie voor veel bedrijven geen haalbare oplossing.

Recovery-in-place and DRaaS

De situatie is volledig veranderd dankzij ontwikkelingen in de wereld van virtuele serverback-ups en cloud computing. Tegenwoordig kunnen gebruikers hun toepassingen uitvoeren vanaf image based back-ups van virtuele machines. Deze mogelijkheid wordt ‘recovery-in-place’ of ‘instant-recovery’ genoemd. Door recovery-in-place wordt de RTO significant verbeterd doordat de werknemers kunnen doorwerken terwijl de primaire servers worden hersteld. Ook de RPO wordt verminderd. Incrementele snapshot back-ups met een interval van 15 minuten zijn namelijk erg gebruikelijk. De images van virtuele machines kunnen ook naar een andere locatie of naar de cloud worden gekopieerd voor hersteloperaties.

Er zijn verschillende manieren om dit soort systemen te implementeren. Veel back-up softwareproducten zijn tegenwoordig in staat om deze taken uit te voeren. Je kunt ook zelf zo’n systeem opzetten als jouw huidige back-upsoftware dit ondersteunt. Als je gebruik maakt van oudere back-up software of als je vanaf nul moet beginnen, kan je er ook voor kiezen om dit werk uit te besteden. Bij dit model wordt er doorgaans een apparaat op de bedrijfslocatie geplaatst voor lokale backup en herstel. De data worden naar de cloud gekopieerd voor hersteloperaties. Met recovery-in-place kan je na een uitval of incident uw toepassingen uitvoeren vanaf dit lokale apparaat of via de cloud. Dit wordt ook wel ‘cloud disaster recovery’ of ‘disaster recovery as a service’ (DRaaS) genoemd.

Met DRaaS krijg je de herstelmogelijkheden van traditionele replicatie op afstand, maar dan goedkoper. Gebruikers betalen doorgaans een bepaald bedrag per maand op basis van de hoeveelheid data die in de cloud moet worden opgeslagen.

Soms worden er extra kosten in rekening gebracht vanwege de benodigde verwerkingskracht om de toepassingen tijdens hersteloperaties in de cloud uit te kunnen voeren. Als we die kosten vergelijken met de kosten van de faciliteiten, het personeel en de technologie bij het opzetten van een tweede datacenter, wordt de waarde van recovery-in-place en DRaaS al snel duidelijk.

Verder is het belangrijk om jouw IT-herstelplan te testen. Vroeger was dit lastig en mogelijk zelfs riskant. Dankzij de huidige technologieën en diensten is het testproces echter veel gemakkelijker geworden. Omdat het zo eenvoudig is om virtuele servers te maken, kunnen er herstel testomgevingen worden opgezet zonder dat de productiesystemen beschadigd raken. Er zijn zelfs DRaaS-providers die zelf de hersteltests voor hun klanten uitvoeren.

4.Houd Je Bedrijf Draaiende

Zoals gezegd hebben veel bedrijven tegenwoordig maar weinig ruimte voor downtime. Als jouw werknemers of klanten geen toegang hebben tot essentiële toepassingen en data, heeft dit een directe weerslag op de productiviteit en dus de omzet.

Dat klinkt misschien logisch, maar veel organisaties houden geen rekening met de daadwerkelijke kosten van downtime voor hun bedrijf. Laten we kijken naar het volgende voorbeeld, waarbij we gebruikmaken van de RTO-calculator van Datto, om je een beter beeld te geven van de kosten van downtime.

We gaan ervan uit dat jouw bedrijf 100 werknemers heeft en dat de gemiddelde omzet per uur op een normale dag € 1500 is. Om hun dagelijkse taken uit te kunnen voeren,

moeten de werknemers toegang hebben tot hun e-mail, een grote database en verschillende bestanden. Laten we ervan uitgaan dat deze data in totaal 2 TB is, dat je op jouw locatie iedere dag om 18.00 een incrementele back-up uitvoert en dat deze back-up ook naar een cloudback-upservice wordt gekopieerd.

Met deze parameters zou het volledige herstel van een lokale back-up 8,5 uur duren. De downtime zou jouw organisatie € 34.000 aan verloren omzet kosten.

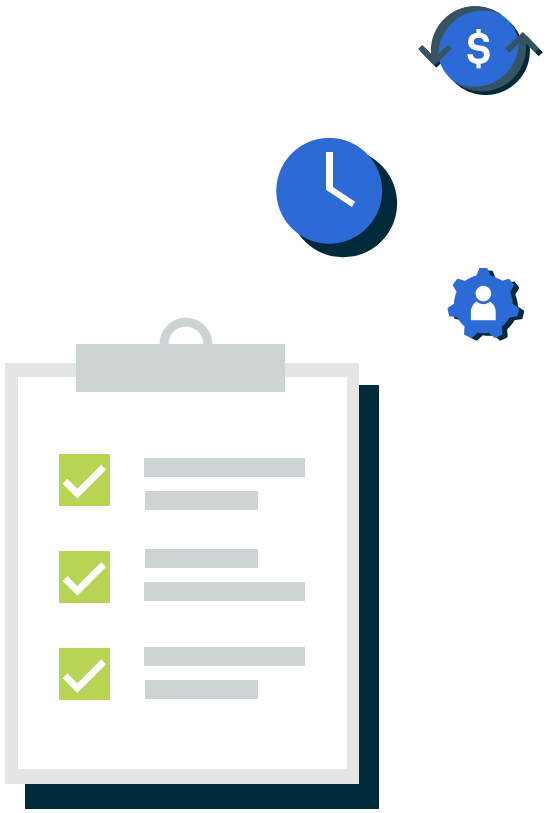
Het wordt nog erger als die 2 TB data moet worden hersteld vanuit een cloudbackup service. Dan zou het 6 dagen, 9 uren en 42 minuten kunnen duren om diezelfde 2 TB via het internet vanuit een cloudservice te herstellen. De verloren omzet zou jouw bedrijf dan € 614.800 kosten. Deze getallen verschillen natuurlijk per bedrijf, maar dit voorbeeld geeft duidelijk aan dat het belangrijk is om te kunnen blijven doorwerken terwijl de primaire servers en opgeslagen data worden hersteld.

Bedrijfscontinuïteit

De downtime van toepassingen is natuurlijk slechts een van de factoren die van invloed zijn op jouw bedrijfsresultaat. Ook hier zijn er veel verschillende zaken waarmee je rekening moet houden, afhankelijk van de grootte en de aard van jouw organisatie. Er zijn echter een paar factoren die voor veel bedrijven gelijk zijn.

Verzekeringen—Verzekeringen spelen bij hersteloperaties een belangrijke rol. Stel dat jouw bedrijf bijvoorbeeld over veel magazijnen beschikt, gevuld met goederen die op ieder moment gedistribueerd moeten kunnen worden. Bij een brand of overstroming zou het erg veel geld kosten om de goederen te vervangen en zouden de gevolgen voor jouw onderneming groot zijn. Daarom is het essentieel om de juiste dekking te kiezen die aansluit op de specifieke behoeften van jouw bedrijf. Het is ook erg belangrijk om alle verzekeringsinformatie goed te documenteren, zoals het polisnummer, jouw aanmeldgegevens, de procedure om claims in te dienen, enz.

Met DRaaS krijg je de herstelmogelijkheden van traditionele replicatie op afstand, maar dan goedkoper.



Training—Bij ieder bedrijf moet worden uitgezocht welke werknemers onmisbaar zijn voor het herstelproces. Dit kunnen bijvoorbeeld leidinggevenden, afdelingsmanagers of IT-medewerkers zijn. Vervolgens moet je bepalen wat voor functies en verantwoordelijkheden zij hebben als het gaat om bedrijfscontinuïteit, wat de structuur van jouw bedrijf ook is. Het is ook van belang dat jouw werknemers de essentiële taken van anderen leren voor het geval dat een onmisbare collega na een incident niet in staat is om te werken.

Faciliteiten—Het is belangrijk om de faciliteit(en) te evalueren waarin de bedrijfsoperaties worden uitgevoerd. Hierbij moet je onder andere rekening houden met de volgende punten:

- Adequate brandbestrijdingssystemen
- Generatoren die de essentiële apparatuur van stroom kunnen voorzien
- Noodstroomvoedingssystemen voor kritische servers
- Overspanningsbeveiligingssystemen
- Alarm-/intercomsystemen om werknemers te waarschuwen in noodsituaties

Afhankelijkheid—Het is cruciaal om rekening te houden met alle partijen van wie je afhankelijk bent, zowel binnen als buiten jouw organisatie. Stel dat jouw bedrijf medische hulpmiddelen produceert. Het kan zijn dat je de onderdelen van verschillende leveranciers krijgt, misschien zelfs uit andere landen. Stel dat een van deze leveranciers te maken krijgt met een overstroming of brand en de productie wordt stopgezet. Hierdoor kun je mogelijk niet meer de benodigde onderdelen krijgen, wat directe gevolgen heeft voor jouw bedrijfsoperaties. In jouw bedrijfscontinuïteitsplan moeten oplossingen staan om deze problemen in te perken, bijvoorbeeld door meerdere leveranciers te gebruiken of een grote hoeveelheid essentiële onderdelen in te slaan.

Conclusie

Een plan voor bedrijfscontinuïteit en hersteloperaties zou voor alle bedrijven een essentieel aspect moeten zijn. Veel organisaties denken er echter helemaal niet over na. Andere organisaties hebben wel een plan, maar weten niet goed hoeveel tijd het herstelproces kost en hoeveel geld downtime kost. Het goede nieuws is dat de huidige databeveiligingstechnologieën en -diensten het IT-stukje van de bedrijfscontinuïteitspuzzel enorm hebben verbeterd. Er zijn vandaag de dag veel verschillende mogelijkheden beschikbaar met verschillende prijskaartjes. Hierdoor kan je een product of dienst uitkiezen waarmee in de specifieke behoeften van jouw bedrijf wordt voorzien.

Zoals je wellicht hebt gemerkt, hebben we het in dit e-book ook veel gehad over het testen van jouw plannen. Het belang van het testen van plannen voor bedrijfscontinuïteit en hersteloperaties mag zeker niet worden onderschat. Testen is de enige manier om de gaten in jouw plannen op te sporen en te dichten. Deze gaten wil je natuurlijk niet pas tegenkomen wanneer je met alle macht de situatie onder controle probeert te krijgen, wanneer na een wolkbreuk de receptie onder water staat.

FASTBYTE

Maakt ICT behapbaar