Ministerie van Economische Zaken
en Klimaat

Adviezen voor het maken van een back-up

Inrichten van een kwalitatief goede back-up

Als organisatie ben je vaak afhankelijk van IT-systemen voor (kritieke) bedrijfsprocessen en voor het opslaan van data. Wanneer deze bedrijfsprocessen verstoord raken of belangrijke data verloren gaan, kan dit grote gevolgen hebben voor een organisatie. Daarom is het hebben van een back-up van groot belang. Ook van belang is dat de kwaliteit van de back-up op orde is.

Wat is een back-up?

Wanneer we praten over een back-up hebben we het eigenlijk over het maken van een kopie van de originele data die opgeslagen staan op een apparaat. Mocht er wat gebeuren met het origineel dan ben je daar niet meer volledig van afhankelijk en kun je dit door middel van de back-up weer herstellen. Doordat we steeds meer opslag nodig hebben voor onze data, groeit ook de opslag die nodig is voor de kopie van deze data. Aanbieders van back-up software gebruiken om deze reden steeds nieuwere technieken om een kopie van al deze data te kunnen maken. De cloud speelt een steeds grotere rol in data-opslag van back-ups omdat de data dan op een andere plek bewaard worden.

Risico's

Om er voor te zorgen dat belangrijke data en systemen niet verloren gaan, is het belangrijk om een back-up te hebben. Het nut van een back-up merk je in de praktijk vaak alleen wanneer een incident optreedt met dataverlies als gevolg. Om deze reden wordt een back-up soms alleen gezien als een vervelende kostenpost met als gevolg dat er niet altijd voldoende aandacht aan wordt besteed. Dit kan er voor zorgen dat een back-up niet voldoet wanneer je deze nodig hebt.

digital trust
center.

Adviezen voor het maken van een back-up

Voor het inrichten van een kwalitatief goede back-up binnen je organisatie kun je het beste een strategie opstellen. Soms kan het handmatig kopiëren van bestanden naar een externe harddisk al volstaan als een goede vorm van back-up. Het is echter aan te raden om een back-up te automatiseren, zodat je het maken van een back-up niet kunt vergeten. Als je een goede back-up wilt maken zijn de volgende punten van belang. Ook wanneer de IT is uitbesteed bij een dienstverlener, kun je deze punten bespreken en eventueel meenemen in een Service Level Agreement (SLA).

Onderstaande tips bieden handvatten voor het maken van een **kwalitatief goede back-up**.

Retentie van de back-up

De zogenoemde retentie van een back-up geeft aan hoe ver je terug kan in de geschiedenis van een back-up. Dit kan van belang zijn wanneer je bijvoorbeeld een bestand terug wil zetten wat een jaar geleden is verwijderd. In dat geval zou een backup die een retentie van een maand heeft geen oplossing bieden.

Een langere retentie zal meer opslag vergen waardoor een onbeperkte retentie misschien 'handig om te hebben' klinkt, maar kan wel onnodig in de kosten oplopen. Let hierbij ook op wettelijke afwegingen, de wet kan soms voorschrijven hoe lang data bewaard moet worden.

Locatie & Media van de back-up

Idealiter richt je een back-up in volgens de "3-2-1 Methode". Deze methode stelt dat je minimaal 3 kopieën van je data hebt, die je op 2 verschillende media zet en waarvan 1 op een andere locatie wordt opgeslagen.

Bij verschillende media kan gedacht worden aan een harddisk, tape, of cloud opslag. Het type media kan helpen bij het bepalen van de locatie, maar heeft vaak te maken met de hoeveelheid data die opgeslagen dient te worden. Bedenk ook dat de ruimte die een back-up nodig heeft meestal groeit in de loop van tijd. Dit is sterk afhankelijk van de retentie en frequentie van back-ups.

Toegang & Beveiliging van back-up

Het is belangrijk om na te denken hoe je back-ups beschermt op het gebied van toegang. Mocht bijvoorbeeld een back-up media gestolen worden dan kun je deze door middel van encryptie beveiligen om er voor te zorgen dat deze niet in te zien zijn.

Denk ook na wie er binnen je organisatie toegang mag krijgen tot de back-ups. Dit geldt zowel fysiek als via back-up software. Wanneer je normaal gesproken een rechtenindeling hebt om niet alle data voor iedereen inzichtelijk te maken, zou iemand middels verkregen toegang deze data wel kunnen benaderen.

Frequentie back-up

Bij het bepalen van de frequentie van de back-up moet je rekening houden met de data die verloren kan raken bij een incident. Mocht je bijvoorbeeld om 16:00 uur worden getroffen door ransomware en je back-up draait 's nachts om 03:00 uur, dan ben je mogelijk een aantal uur aan werk kwijt. Deze afweging heet 'Recovery Point Objective' (RPO).

Het verhogen van de frequentie zou kunnen helpen bij het verkleinen van het aantal uur aan werk dat mogelijk verloren gaat bij zo'n incident. Een hogere frequentie van de back-up is niet altijd mogelijk vanwege de tijd die het kost om de back-up te maken of de vertraging die mogelijk optreedt terwijl deze draait.

Hersteltijd

Wanneer een incident plaatsvindt waardoor (kritieke)bedrijfsprocessen worden geraakt, is het belangrijk om te weten hoe lang het duurt voordat je data en applicatie(s) weer beschikbaar. Meerdere factoren hebben impact op de hersteltijd zoals de hoeveelheid data, de gebruikte techniek of de snelheid van de back-up media. Het kan zijn dat je afwegingen moet maken wat je wanneer herstelt om zo snel mogelijk weer aan het werk te kunnen. Deze afweging heet 'Recovery Time Objective' (RTO). Binnen zo'n afweging zul je soms prioriteiten moeten stellen zodat belangrijke onderdelen eerder hersteld worden dan andere.

Het stellen van prioriteiten kan ook helpen bij het beperken van de kosten doordat je misschien hebt bepaald dat actieve projecten wel binnen een aantal uur weer beschikbaar moeten zijn, maar een archief bijvoorbeeld pas na een aantal dagen.

Back-up monitoren

Wanneer de back-up is ingeregeld, is het ook van belang dat je de back-up monitort. Zorg dat je over goede rapportage beschikt waarmee je, het liefst dagelijks, kunt nagaan of back-ups daadwerkelijk draaien en of er geen fouten zijn opgetreden. Het is belangrijk dat eventuele fouten tijdig worden hersteld zodat je hier niet tegen aanloopt wanneer je een back-up nodig hebt. Ook wanneer je het volledig hebt uitbesteed, is het nog steeds belangrijk dat je als ondernemer deze rapportages ontvangt en controleert.

Testen back-up

Naast het monitoren van back-ups is het misschien nog wel belangrijker dat ze getest worden. Het testen van back-ups wordt soms alleen gedaan wanneer er daadwerkelijk iets hersteld moet worden. Dit heeft er mede mee te maken dat het testen vaak geld en veel tijd kost. Sommige back-up applicaties bieden de mogelijkheid om een verificatietest te draaien. Zo'n verificatietest kijkt of de back-up data in orde zijn. Dit is goed om in te richten, maar het liefst ga je een stap verder en test je periodiek de back-up door hem te herstellen zodat je zelf kunt nagaan of het werkt en de data intact zijn. Je kunt een hersteltest doen door steekproefsgewijs wat bestanden te herstellen, of zelfs een geheel systeem te herstellen om ook de functionaliteit van applicaties te testen.

Segmenteren

Wees er van bewust dat het belangrijk is om goede segmentatie toe te passen als het over je back-up gaat. Dit kun je deels al doen met de genoemde 3-2-1 methode waarbij je verschillende media gebruikt. Probeer in wat grotere omgevingen, waar mogelijk ook gebruik wordt gemaakt van virtualisatie, het backup netwerk en het productie netwerk te scheiden. Uit recente gerichte (ransomware-) aanvallen blijkt dat er veel energie wordt gestoken om ook de back-ups te versleutelen. De enige optie om je data mogelijk terug te krijgen, is dan het betalen van losgeld. In de praktijk blijkt dat onvoldoende segmentatie er voor zorgt dat ook de back-up makkelijk versleuteld kan worden.

Kijk voor meer informatie op www.digitaltrustcenter.nl