Hoe vaak moet ik een backup maken van mijn bedrijfsdata?

https://aucuba.nl/kennisbank/uncategorized/hoe-vaak-moet-ik-een-backup-maken-van-mijn-bedrijfsdata/

Voor de meeste MKB-bedrijven geldt dat een dagelijkse backup van bedrijfsdata de minimale standaard is. Hoe vaak je precies een backup moet maken, hangt af van hoe snel jouw data verandert en hoeveel dataverlies jouw bedrijf kan opvangen zonder ernstige gevolgen. In dit artikel beantwoorden we de meest gestelde vragen over backupfrequentie, backupstrategie en hoe je jouw bedrijfsdata optimaal beschermt.

Wat gebeurt er als je bedrijfsdata verloren gaat?

Als bedrijfsdata verloren gaat, kan dat leiden tot operationele stilstand, financiële schade en reputatieverlies. Zonder een werkende backup ben je afhankelijk van wat er nog op individuele apparaten staat, en dat is in de meeste gevallen onvolledig of verouderd. Herstel zonder backup is tijdrovend, kostbaar en soms simpelweg onmogelijk.

Denk aan situaties als een ransomware-aanval die bestanden versleutelt, een medewerker die per ongeluk een cruciale map verwijdert, of een harde schijf die plotseling uitvalt. In al deze gevallen bepaalt de aanwezigheid van een recente backup hoeveel werk je kwijt bent en hoe snel je weer operationeel bent. Voor bedrijven zonder interne IT-afdeling is dit risico extra groot, omdat er vaak geen gestructureerd dataherstelplan klaarligt.

Naast de directe schade zijn er ook indirecte gevolgen: klanten die wachten op offertes, facturen die niet verzonden worden, projecten die stilliggen. De impact groeit naarmate dataverlies langer onopgemerkt blijft of herstel meer tijd kost.

Hoe bepaal je de juiste backupfrequentie voor jouw bedrijf?

De juiste backupfrequentie voor jouw bedrijf bepaal je aan de hand van twee sleutelvragen: hoeveel data kan jouw bedrijf verliezen zonder grote gevolgen, en hoe snel verandert jouw data? Dit wordt ook wel de Recovery Point Objective (RPO) genoemd. Hoe korter de RPO, hoe vaker je een backup moet maken.

Een administratiekantoor dat dagelijks tientallen facturen verwerkt, heeft andere eisen dan een bedrijf dat wekelijks een paar documenten aanpast. Stel jezelf de vraag: als de systemen morgenochtend uitvallen, hoeveel werk wil je dan maximaal opnieuw doen? Is dat een uur, een dag, of een week? Het antwoord bepaalt direct hoe vaak je een backup maakt van jouw bedrijfsdata.

Andere factoren die meewegen zijn de sector waarin je actief bent, eventuele wettelijke bewaarplichten voor bepaalde gegevens, en de hoeveelheid data die dagelijks wordt aangemaakt of gewijzigd. Een backupstrategie voor MKB-bedrijven hoeft niet complex te zijn, maar moet wel afgestemd zijn op de realiteit van jouw bedrijfsprocessen.

Wat is het verschil tussen dagelijkse, wekelijkse en realtime backups?

Het verschil zit in hoe recent de opgeslagen data is op het moment dat er iets misgaat. Een dagelijkse backup bewaart de stand van zaken van de vorige nacht, een wekelijkse backup kan tot zeven dagen aan werk kosten bij verlies, en een realtime backup slaat wijzigingen vrijwel direct op zonder noemenswaardige vertraging.

Dagelijkse backup

Een dagelijkse backup is voor de meeste MKB-bedrijven de praktische standaard. Bestanden worden elke nacht automatisch opgeslagen, zodat je bij een incident maximaal één werkdag aan data kwijt bent. Dit is een goed evenwicht tussen bescherming en beheerbaarheid.

Wekelijkse backup

Een wekelijkse backup volstaat alleen voor data die zelden verandert, zoals archiefdocumenten of jaarverslagen. Voor actieve bedrijfsprocessen is dit vrijwel altijd onvoldoende. Het risico op aanzienlijk dataverlies is te groot voor de meeste operationele omgevingen.

Realtime backup

Realtime of continue backup slaat wijzigingen direct op, soms tot op de minuut nauwkeurig. Dit is ideaal voor bedrijven met kritieke systemen zoals een webshop, boekhoudsoftware of klantendatabase die continu wordt bijgewerkt. De technische vereisten en kosten zijn hoger, maar de bescherming is maximaal.

Wat is de 3-2-1 backupregel en hoe pas je die toe?

De 3-2-1 backupregel is een beproefde standaard voor een betrouwbare backupstrategie: bewaar drie kopieën van je data, op twee verschillende opslagmedia, waarvan één kopie zich buiten je kantoor bevindt. Deze aanpak beschermt je tegen vrijwel elk scenario van dataverlies, van hardwarefalen tot brand of diefstal.

In de praktijk ziet dit er voor een MKB-bedrijf vaak zo uit: de originele data staat op de werkcomputers of server, een tweede kopie staat op een externe harde schijf op kantoor, en een derde kopie wordt automatisch opgeslagen in de cloud. De cloudbackup zorgt ervoor dat je bij een fysieke calamiteit op kantoor altijd nog een recente kopie hebt die buiten het pand bewaard wordt.

De 3-2-1 regel is geen garantie op zichzelf. Het gaat erom dat de kopieën ook daadwerkelijk actueel zijn en regelmatig worden getest. Een backup die maanden oud is of niet herstelbaar blijkt, biedt weinig bescherming in een noodsituatie.

Hoe weet je of je backup daadwerkelijk werkt?

Je weet of je backup werkt door hem regelmatig te testen via een hersteltest. Een backup die nooit getest is, is geen betrouwbare backup. Veel bedrijven ontdekken pas bij een incident dat hun backupbestanden beschadigd zijn, onvolledig zijn opgeslagen of niet meer leesbaar zijn.

Een hersteltest houdt in dat je een of meerdere bestanden terugzet vanuit de backup naar een testomgeving en controleert of ze volledig en bruikbaar zijn. Dit hoeft niet wekelijks te gebeuren, maar minstens eens per kwartaal is verstandig. Voor kritieke systemen is maandelijks testen aan te raden.

Controleer daarnaast regelmatig de backuplogboeken. Moderne backupsoftware geeft meldingen als een backup mislukt of als er onverwachte fouten optreden. Wie deze meldingen negeert, loopt het risico maanden zonder werkende backup te zitten zonder het te weten. Wij helpen klanten bij het opzetten van proactieve monitoring zodat dit soort fouten direct worden opgemerkt.

Welke bedrijfsdata moet je sowieso altijd backuppen?

Bedrijfsdata die je sowieso altijd moet backuppen is data die bij verlies direct operationele of financiële schade veroorzaakt of wettelijk bewaard moet worden. Dit omvat financiële administratie, klantgegevens, contracten, projectbestanden en e-mailcommunicatie.

Concreet gaat het om de volgende categorieën:

- **Financiële administratie:** facturen, offertes, boekhouding en belastingdocumenten
- **Klant- en relatiegegevens:** contactinformatie, contracten en correspondentie
- **Projectdocumentatie:** planningen, rapporten, tekeningen of specificaties
- **Personeelsgegevens:** arbeidsovereenkomsten, salarisadministratie en HR-dossiers
- **Bedrijfskritieke software-instellingen:** configuraties van systemen die je dagelijks gebruikt

Let er ook op dat data in cloudapplicaties zoals Microsoft 365 of Google Workspace niet automatisch volledig beschermd is. De aanbieder zorgt voor de beschikbaarheid van de dienst, maar niet altijd voor herstel van verwijderde of overschreven bestanden na een langere periode. Een aparte backup van clouddata is daarom verstandig.

Moet je kiezen tussen lokale opslag of cloudbackup?

Je hoeft niet te kiezen tussen lokale opslag of cloudbackup. De sterkste backupstrategie voor MKB-bedrijven combineert beide. Lokale opslag biedt snelle toegang en snel herstel bij kleine incidenten, terwijl cloudbackup beschermt tegen fysieke schade aan het kantoor en op afstand toegankelijk is.

Lokale opslag, zoals een NAS-server of externe harde schijf, maakt het mogelijk om grote hoeveelheden data snel terug te zetten zonder afhankelijk te zijn van een internetverbinding. Dat is praktisch als een medewerker per ongeluk een map verwijdert en die dezelfde dag nog nodig heeft.

Cloudbackup biedt geografische spreiding. Als er iets misgaat op kantoor, brand, overstroming of inbraak, staat jouw data veilig op een externe locatie. Bovendien schalen cloudoplossingen mee met de groei van jouw bedrijf, zonder dat je zelf extra hardware hoeft aan te schaffen. De keuze voor een specifieke cloudoplossing hangt af van factoren als de hoeveelheid data, de gewenste hersteltijd en de eisen vanuit jouw branche.

Twijfel je over welke aanpak het beste past bij jouw bedrijf, of wil je weten of jouw huidige backupstrategie voldoende is? Neem gerust contact met ons op. We denken graag met je mee en zorgen voor een oplossing die aansluit bij jouw situatie.