backupdagen 31. mars

# Det du må vite om backup i skyen: Veiledning til kostnad, sikkerhet og fleksibilitet

WHITEPAPER

## Utfordringene

Behovet for robuste backup- og gjenopprettingssystemer har aldri vært viktigere enn i dag. Datavekst fortsetter med uforminsket styrke og ifølge IDC, opprettes og gjenskapes datamengden globalt i form av e-post, direktemeldinger, dokumenter, videoer og sosiale nettverk og vil overstige 35 billioner gigabyte i 2020.

For å komplisere det ytterligere, har eierstyring, selskapsledelse og industrilovgivning gjort ledere ansvarlige for sikkerheten til bedriftsinformasjonen, og tvinger dem til å oppgi bevis på aktsomhet og flid om hvordan data er lagret. Samtidig omformes utseendet til forretninger via virtualisering og data i skyen. Mens disse initiativene lover større effektivitet og kostnadsbesparelser, må man vurdere hvordan de påvirker og integriteten av en organisasjons data. På grunn av dette må IT-sjefer sette seg nøye inn i selskapets forretningsmodell og aktivt delta i strategiske prosesser som påvirker datasystemene.

## Løsningene som må vurderes

I løpet det siste tiåret har cloud backup og restore dukket opp som en sikker, kostnadseffektiv og pålitelig metode for å ivareta den økende mengden bedriftsinformasjon som daglig genereres. Å bytte til et cloud-basert backupløsning er en betydelig avgjørelse som krever en tydelig forståelse av hvordan en slik løsning integreres i bedriften din. Dette whitepaper tar for seg de vanligste spørsmålene som bedrifter lurer på angående cloud backup og vil hjelpe deg med å avgjøre hvilken rolle en cloud backup og restoreløsning kan ha for bedriften din.

---

## Avsnitt A: Utforsking av cloud.

### Hva betyr offentlig, privat og hybrid cloud?

Skillet mellom ulike cloud-modeller vil hjelpe deg med å avgjøre hvilken type backupløsning organisasjonen trenger. En offentlig cloud er en administrert løsning som involverer et eksternt datasenter som kan tilby fleksibilitet og skalerbarhet for behandlings- og lagringsbehov. En privat cloud oppstår når et selskap bygger og forvalter sitt eget datasenter som styres bak et selskapets brannmur. En hybrid cloud tilbyr en blandet tilnærming til infrastruktur som linker sammen to unike datasentre, et privat og et offentlig.

Med en offentlig cloud bør backupløsningen optimalisere datainnsamlingen og lagringen for å bidra til å minimere båndbreddens krav til bedriftens nettverk. Man bør kunne forvente at en leverandør av backup og restoretjenster i cloud har programvare og infrastruktur. Service, support og kompetanse må være en del av leverandørens dokumenterte SLA.

Enten med en privat eller en hybrid cloud, kan det være nødvendig med en leverandør for å kunne gi bedriften riktig programvare-plattform til å administrere backup i den private skyen. Hvis det gjelder en hybrid cloud, vil bedriften ha valget mellom å bytte mellom et privat datasenter og et cloud-basert lagringsalternativ, og hvilket backup-behov du har.

## Hvorfor backup og gjenoppretting i cloud?

Backup og restore gir deg en kostnadseffektiv, sikker og pålitelig metode for å sikkerhetskopiere og gjenopprette kritiske data — livsnerven i bedriften din. Systemet gjenoppretter data uansett hvor du befinner deg, også individuelle filer i opprinnelig format slik at du kan gjenoppta driften umiddelbart. Det gir deg også en fleksibel løsning som skalerer når lagringskapasiteten må utvikles i takt med bedriftens vekst.

## Hva er vanligste fremgangsmåte for å gjennomføre backup og restore i cloud?

Hver cloud backup-løsning er unik, da den tar hensyn til de spesielle behovene for databeskyttelse for organisasjonen din. Dette kan omfatte eksterne kontorer, bærbare datamaskiner og mobile enheter som nettbrett og smarttelefoner. Eventuelle komplikasjoner involvert i å flytte til en outsourced cloud backup-tjeneste kan reduseres ved å velge riktig tjenesteleverandør for backup. Leverandøren må kunne tilby en løsning som er agnostisk når det gjelder både maskinvare og programvare slik at du kan utnytte eksisterende infrastruktur. Å velge riktig tjenesteleverandør vil gi deg en garantert problemfri gjennomføring og kontinuerlig support ved behov.

Konkurranseutsetting av trivielle backup-prosesser til en velprøvd backup-ekspert i cloud vil gjøre deg i stand til å re-distribuere eksisterende IT-ressurser til mer strategiske inntektsgenerende tiltak.
Din tjenesteleverandør for backup i cloud vil veilede deg gjennom implementeringsprosessen og gi dedikert support for å hjelpe deg å kalibrere og optimalisere backup-løsningen for deg.

Den gode nyheten er at når din private backup og gjenopprettingsløsning i cloud er på plass, vil det kreve minimalt med vedlikehold sammenlignet med on-site-løsninger, som tape-backup eller disker. Det er avgjørende at din leverandør av cloud backup har vist ekspertise i å levere trygge backup-løsninger. En grundig testet gjennomføring vil forsikre bedriften din om at en backup-løsning i skyen ikke vil svikte når det er størst behov. Datasystemet med all elektronisk informasjon representerer store verdier, kanskje den største i selskapet.

## Hvordan betjenes vanligvis datagjenoppretting med en cloud-modell?

To viktige faktorer i forståelsen av datagjenoppretting er Recovery Time Objectives (RTO) og Recovery Point Objectives (RPO). RTO refererer til hvor raskt bedriften din har behov for gjenoppretting etter tap av data og kan måles i timer eller dager. RPO refererer til hvor mye data bedriften din tåler å tape og måles i timer. For eksempel kan et Fortune 500-firma for noen typer data kreve en RTO på fem timer og en RPO på en time. RPO og RTO kan variere for ulike typer data.
Hver bedrift har behov for å bestemme RTO og RPO basert på egne beregninger av risikotoleranse og krav til driftskontinuitet.

Som en del av denne prosessen, er det viktig å se godt på den type data som bedriften samler inn og bruker på en time, daglig eller ukentlig basis. Mange bedrifter klarer ikke å innse hvor viktig rask restore er for å oppnå forretningsmessige mål — helt til de opplever alvorlige tap av data.

Virkningen av datatap kan være betydelig. En detaljhandel, for eksempel, samler stadig inn data for å utføre analyser knyttet til prisstrategier, lagerforsyning og perioder med etterspørsel. Disse data i sanntid er avgjørende for å være konkurransedyktig.

Mange firmaer har ikke lenger råd til å stole på at en lastebil ankommer hver dag for å ta tape-backup offsite fordi det potensielt setter en hel dagsjobb av verdifull konkurransedyktig forretningsdata i fare.

# Avsnitt B: Å forstå sikkerhet med backup i cloud

## Hvordan kan jeg sikre at mine krav til tilgjengelighet oppfylles når bedriftens data lagres eksternt i en cloud?

Bedriften din vil fortsette å påta seg ansvar for datasikkerhet, selv ved bytte av backup-ansvar til en leverandør for cloud backup. Du bør forvente at tjenesteleverandøren kan fortsette å holde på en lokal kopi av dine siste backup i tilfelle du kobles fra nettskyen. Leverandøren for backup i cloud må også vise at den har flere datasentre for å sikre at dine data beskyttes av en passende mengde overflødighet av infrastruktur.

Disse datasentrene bør også være geografisk fordelt på to forskjellige lokasjoner for å kunne øke sikkerheten i tilfelle av en naturkatastrofe eller strømbrudd. Sammen med en Disaster Recovery Plan, bør leverandøren også være i stand til å demonstrere en Business Continuity Plan som beskriver hvordan den vil håndtere en rekke situasjoner.

## Hvordan garanterer et backup-system i cloud at data overføres sikkert?

Alle data blir komprimert og deduplisert før det sendes kryptert gjennom cloud til et datasenter. Data forblir kryptert på backupserverne. Eneste nøkkel for dekryptering ligger hos deg, og sikrer at backup og gjenopprettingsløsning i skyen er så trygg og sikker som lokal backup og gjenopprettingssystem for data.
Siden bedriftens data skal overføres via internett, er krypteringsstandarden som brukes av leverandøren svært viktig.

Leverandøren bør bruke Advanced Encryption Standard (AES) sammen med FIPS 140-2 sertifisering, noes om validerer tredjepart fra National Institute of Standards and Technology (NIST). FIPS 140-2 er høyeste nivå av klarert sertifisering av tredjepart og indikerer at krypteringen er riktig gjennomført på en måte som ikke kan beseires.

## Hvilke forsikringer må jeg se etter for å sikre en trygg cloud backup-tjeneste?

Bedriften din må utføre en due diligence for å sikre at leverandøren av cloud-backup dekker dine forretningsbehov. Grunnleggende spørsmål inkluderer: hvor lenge har leverandøren vært i bransjen og yter de for tiden tjenester som ligner på din, i form av vertikalt marked, størrelse og omfang. Avhengig av dine samsvarskrav, bør leverandøren for cloud-backup være kjent med relevant industriterminologi og standarder som påvirker bedriften din.

En av de vanligste metodene for å sikre at forventningene dine oppfylles, er gjennom en sterk Service Level Agreement (SLA). Dette dokumentet vil skissere ønskede driftsnivåer og beskrive konsekvensene hvis SLA ikke oppfylles. SLA bør også gi deg en forsikring om at leverandøren for cloud-backup er en troverdig, trygg forretningspartner som har sertifiseringer som gjør det mulig å opprettholde samsvarskravene.
Sammen med en SLA bør leverandøren du har valgt ta hensyn til en sluttavtale.

En leverandør for backup-tjenester som låser deg til en langsiktig kontrakt har mindre motivasjon for å tilby høye nivåer av kundesupport enn leverandører som må møte periodiske fornyelser. Ikke bli låst inn i en hvilken som helst cloud eller leverandør for cloud backup. Leverandøren for cloud backup bør gi deg fleksibilitet til å flytte fra en privat eller hybrid sky til en offentlig sky-plassering hvis bedriftens behov endres over tid.

Dessuten er leverandøren for cloud backup bare forvalteren av dine data, du eier og kontrollerer dine data.

Leverandøren plikter å gi deg rimelig tilgang til dine data med assistanse til å overføre data andre steder ved behov. For eksempel, hvis du vil flytte penger fra en bank til en annen, er det ingen lås på de og heller ingen straff for å flytte egne eiendeler. Samme omstendigheter bør gjelde for leverandøren av cloud backup.

## Hvilket nivå av IT-ressurser er nødvendig for å angi og vedlikeholde en backup-løsning i cloud?

For de fleste bedrifter vil en cloud backup og gjenopprettingsløsning eliminere, eller redusere IT-ressurser relatert til den kjedelige oppgaven av backup og omplassere ressursene dine til mer strategiske prosjekter. Å jobbe med en pålitelig leverandør for cloud backup gjør at du kan utnytte din eksisterende nettverksinfrastruktur ved overføring av ansvar for backup til en ekstern ekspert.

Dette kan være enda viktigere med tanke på utfordringene noen bedrifter møter når de ansetter erfarne IT-administratorer for backup for lokale løsninger, spesielt i mindre byer eller på eksterne geografiske områder. Det gjør også at IT-sjefer kan fokusere på betydelige transformasjonsprosjekter i stedet for implementering av backup, som vanligvis har lavere prestisjeverdi innenfor de fleste organisasjoner.

Når du bestemmer de riktige innstillingene, automatiseres backup og skaper et “angi-det-og-glem-det”-scenario. Du må imidlertid sikre at din leverandør for cloud backup er utstyrt for å overvåke backup for å identifisere og rette opp eventuelle problemer.

Prisen på backup-tjenesten reflekterer hvor mye ansvar du opprettholder versus leverandøren for cloud-backup. Tjenestetilbud med lave kostnader kan bety at du blir utstyrt med marginal support, minimale seniortekniske ressurser og den pågående byrden for overvåking og administrasjon av din backup.

## Sammen med totale eierkostnader, er det andre tilhørende økonomiske fordeler med en sky-backup, inkludert:

- Lavere drifts- og administrasjonskostnader grunnet automatiske backup
- Innebygd skalerbarhet som gjør det lett å utvikle nye forretningsbehov
- Programvare for cloud-backup som skanner dine data for integritets- og korrupsjonsproblemer, og umiddelbart varsler bedriften for dermed å forebygge kostbare problemer i forveien
- Distribusjon av IT-ressurser i mer strategiske, innovative initiativer som muliggjør større konkurransefordeler
- Enkle gjenopprettingsøvelser for sjelefred

## Hvorfor Cloud Backup?

Disse svarene skal gi et bedre bilde av hva overgangen til en cloud backup og gjenopprettingsløsning innebærer. Grunnet påliteligheten, kostnaden, sikkerheten og administrasjonen i forbindelse med cloud backup, flytter nå mange bedrifter inn i skyen. Årsakene er:

- Evne til å utnytte eksisterende infrastruktur — en cloud-backup og gjenopprettingsløsning krever ikke kjøp eller installasjon av kostbart utstyr siden det drar nytte av ditt eksisterende nettverk
- Enkel og lite tidkrevende installasjon — når du velger en backup-plan, lagres bedriftens data automatisk og gir en transparent løsning
- Mangler ved tape-backup —tapebackup er ofte dyre, sårbare for foreldelse og kan mistes eller stjeles når det transporteres eksternt
- Forbedret gjenopprettingstid — ved å bruke en administrert backup-tjeneste, vil hastigheten og påliteligheten på gjenopprettingen reguleres gjennom SLA
- Smartere bruk av IT-løsninger — en cloud backup og gjenopprettingsløsning lar forretningen din omdirigere IT-ressurser til mer presserende utfordringer i organisasjonen
- Backup Lifecycle Management — en cloud-backup og gjenopprettingsløsning som justerer verdien av dine data mot kostnadene for beskyttelse. Siden verdien av dine data avtar over tid, avtar også kostnadene for beskyttelse, og gir deg ytterligere kostnadsbesparelser.

## Om Backupdagen

Backupdagen er et initiativ fra en rekke kommersielle, offentlige og interesseorganisasjoner. Formålet er å gi private og offentlige bedrifter en påminnelse om hvor viktig dette er, samt hvilke konsekvenser det får hvis rutiner svikter og data blir borte. Backupdagen skal gi bred informasjon om ansvar, løsninger, sikkerhet og teknologisk utvikling innenfor fagområdet. Bakupdagen skal være den 31. mars hvert år. Med andre ord lett å huske som dagen før 1. april. Backupdagen skal være tilsvarende den årlige kampanjen for bytte av batterier i brannvarsleren. Alle vet at et ødelagt batteri kan få katastrofale konsekvenser hvis det brenner.

**Les mer på www.backupdagen.no**