Hvordan velge en leverandør for cloud backup

Hvorfor bør du beskytte dine data?

Før eller senere – via skade, uhell eller feil – er det statistisk sannsynlig at du vil miste verdifull data.
Flere studier viser at 2 til 4 % av alle harddisker må byttes ut hvert år. Det er bare en indikasjon på trusselen for hardware feil. Studien så ikke på andre årsaker av tap av data: utilsiktet sletting av filer, virus, hacking, stjålet utstyr eller naturkatastrofer. Spørsmålet er med andre ord hvordan du får dataene dine tilbake, når dem plutselig blir borte?

Alt handler om gjenoppretting.

Mange tror at det viktigste spørsmålet er "Hvilken måte er best å gjøre backup på?" Det er absolutt et kritisk spørsmål, men forretningsdata er selve livsnerven i bedriften din. Du har ikke råd til å bare se på halve ligningen. Spørsmål om restore av data er enda viktigere og rett på sak:

- Finnes det noen tvil om at data jeg har sikkerhetskopiert kan gjenopprettes hvis en krise oppstår?
- Hvor lang tid tar det å få systemet i gang igjen?
- Hvor mye penger taper jeg mens jeg venter på at mine data skal gjenopprettes?
- Pr. time? Pr. dag? Pr. uke?
- Har jeg riktig hjelp hvis jeg trenger det i en nødsituasjon?

Backup er som å ha bilforsikring: Bør du fokusere på forsikringsselskapets pris og hvor lett det er å kjøpe forsikring? Eller bør du fokusere mer på hva som kan skje hvis du faktisk kommer ut for en ulykke – når du virkelig trenger selskapets støtte og et raskt oppgjør? Til syvende og sist er det tillit som gjelder. Tillit til menneskene som gir deg råd om databeskyttelse. Tillit til backup- og restore-prosesser. Tillit til maskin- og program-vare.

Å ta det riktige valget er avgjørende for suksessen din. Vi har tatt for oss de forskjellige løsningene i dette dokumentet for å hjelpe deg med å velge en leverandør til cloud backup som:

- Dekker behovene dine.
- Holder høyt service og support nivå.
- Nøkkelpersonell med god kompetanse.

- Bruker riktig teknologi.
- Tilbyr verdi utover programvaren.

Viktige faktorer ved vurdering av potensielle leverandører for cloud backup.

Ha tillit til leverandøren

- Har leverandøren et godt rykte?
- Hvor lenge har de drevet virksomheten sin?
- Hvor stabil er bedriften deres?
- Hvor mange kunder har de?
- Hva slags kunder har de?
- Er kundene av tilsvarende størrelse og miljø som din bedrift?
- Har leverandøren erfaring i samme eller lignende bransje som din?
- Har leverandøren erfaring med disaster recovery under lignende forhold som i din bedrift?
- Er de kjent med lover og standarder i bransjen din?

Hva slags presse eller anerkjennelse har de fått?

- Er anerkjennelsen kun basert på pris og merkevare, eller på historikk for kundesupport i ved kriser?
- Er presseanerkjennelsen for det meste fra forbruker- eller næringslivs-presse?
- Har de kundeuttalelser på nettsiden sin?
- Hvor lenge har de vært i bransjen?

Stol på leverandørens teknologi

- Hva slags teknologi er leverandørens tjeneste basert på?
- Er det DIY (Do it yourself)? Best for bare bilder og musikk? En såkalt forretningsversjon av en etablert forbrukertjeneste?
- Hvis det er dyrere, er det mer enn jeg trenger?
- Hvis det er “angi det og glem det”, kan jeg virkelig stole på det?
- Hvordan utføres backup og hvordan vil det påvirke min daglige drift?
- Er det fullstendig integrert? Fungerer det godt med operativsystem, applikasjoner og tjenester?
- Vil det fungere godt på programvare eller systemer jeg vil implementere?
- Tilbyr det fullstendig, trinnvis og kontinuerlig databeskyttelse?
- Gjør det testing av datagjenoppretting lett?
- Er det skalerbart ved vekst i selskapet?
- Inkluderer backupen fil-validering?
- Får du løpende oppdatering på kvaliteten på backup?

Er det lett å konfigurere og vedlikeholde?

- Krever det mye teknisk kunnskap eller talent?
- Hvor lang tid tar det å installere, og hva innebærer det?

- Er det nødvendig å installere ekstra programvare som krever teknikertid, avslutning av systemet og omstart?
- Er det support 24x7?
- Krever det mer plass og strøm for ekstra utstyr?
- Hvor godt fungerer løsningen for avdelingskontorer? – bærbare maskiner? PDA og smarttelefoner?
- Tilbyr leverandøren 24/7 rask, fysisk levering av restore-data i tilfelle en nødsituasjon?
- Hva er alternativene for en bare-metal restore?
- Fungerer backup-løsningen godt i et sofistikert IT-miljø med virtualisering?

Tillit til sikkerheten i tjenesten

- Hvordan sikrer leverandøren tjenesten og hvordan dokumenteres det?
- Har produktet blitt testet og sanksjonert av troverdige tredjeparter som myndighetene og organisasjoner?
- Samsvarer tjenesten med lov- og regel-verk og standarder for din bransje?
- Er den sertifisert av en standardorganisasjon for å sikre beskyttelse mot datatyveri?
- Møter den eller overgår den forsikringskravene til bedriften min?
- Hvis nødvendig, kan leverandøren lett overholde en forespørsel om e-oppdagelse?
- Hvordan utfører leverandøren backup og gjenoppretting av data de lagrer?
- Har leverandøren en Disaster Recovery Plan?
- I tilfelle en katastrofe, har de et annet datasenter med duplikatdata som kan byttes øyeblikkelig slik at det ikke blir avbrudd i tjenesten?
- Er leverandørens datasentere geografisk langt nok fra hverandre slik at de ikke rammes av samme katastrofe?
- Har sekundær-senteret samme tekniske nivå som primær-senteret?
- Har leverandøren en Business Continuity plan?

Selv om leverandørens DR-plan beskytter dine data ved en naturkatastrofe, må spørre deg om de under ekstreme forhold kan drive en tjenesten uforstyrret?

Tillit til kontrakten

- Tilbyr leverandøren en Service Level Agreement?
- Er evt. garantiene, straffereaksjonene og regressene som tilbys i SLA tilstrekkelige?
- Kan jeg tilpasse SLA slik at den dekker mine spesifikke behov eller er det en standardkontrakt?
    - Kan jeg forhandle meg frem til mine egne RTO og RPO?
    - Har leverandøren ekspertise for å hjelpe meg med å angi riktige SLA-standarder til bedriften?
- Spesifiserer SLA responstid for å sette i gang gjenoppretting?
- Spesifiserer SLA alle detaljer omkring sikkerhet inkludert annonserte retningslinjer og sertifiseringer?
- Kan jeg forhandle frem en straffereaksjon hvis SLA ikke oppfylles?
    - Hvordan kan ikke-ytelse i SLA måles utenom en data-katastrofe?

    - Hvis leverandøren ikke oppfyller SLA, er straffereaksjonen bare en frafalt månedlig avgift eller er den betydningsfull, f.eks. en avslutningsklausul?
- Lover leverandøren mer enn de kan levere?
- Ingen leverandør kan garantere en bestemt tid for datagjenoppretting uten å ha full kontroll over alle deler av ligningen – maskinvare, datamengde, programvare, personell, prosesser osv.

Tilbyr leverandøren en avslutningsstrategi eller låser teknologien deg inne?

- Hvis du, etter en stund, ikke er fornøyd med leverandøren eller hvis de går konkurs, sitter du fast i en håpløs situasjon? Med andre ord, har de nok tillit til tjenesten og stabiliteten sin til å tilby en avslutningsstrategi som effektivt vil motivere dem til å holde på bedriften sin?
- Tilbys backup-plattformen av mange andre leverandører? Kan du flytte til en annen leverandør uten å flytte dataene til en annen plattform? Hvor vanskelig blir det?
- Kan jeg tilpasse SLA slik at den dekker mine spesifikke behov? (text in the box)

Hvilken backup-løsning er best og hvorfor sikre dine data?

Denne veiledningen er laget for å hjelpe profesjonelle og kommersielle bedrifter å vurdere sine alternativer for å vedta eller oppgradere backup eller gjenopprettingssystem. Selv om det kan virke innlysende hvorfor du bør beskytte dine data med backup, krever en profesjonell tilnærming til planlegging av et forsvar at alle tenkelige trusler er anerkjent og besvart av løsningen du til slutt velger. Katastrofer som tap av data har mange årsaker og hver av dem er for vanlige til å ignorere.

- Menneskelig feil – utilsiktet sletting
- Maskinvarefeil
- Programvarefeil – fil korrupsjon
- Virus
- Hackere
- Tyveri av datamaskiner eller drivere
- Uhell – brann, flom osv.

I tillegg til å planlegge for alle truslene er det også viktig at du forstår at backup bare er halve beskyttelse. Uten en rask og sikker restore-mulighet kan bedriften fortsatt bli alvorlig rammet ved datatap.

Backup- og restore-system for dataene dine er kjernen i planen for forretningskontinuiteten. Hvordan bedriften svarer på datatap vil ha innvirkning på både din økonomiske situasjon og ditt profesjonelle inntrykk utad. Med best mulig backup- og restore-system:

- Vil bedriften din fortsatt drive virksomheten med et minimalt tap av salg og produktivitet etter tap av data..
- Vil bedriftens omdømme vil være intakt når kunder ser hvor raskt og profesjonelt du gjenoppretter fra tap av data (hvis de i det hele tatt oppdager det.)
- Vil bedriften din unngå store utgifter for teknisk support.
- Vil bedriften din være i samsvar med retningslinjer og industristandarder.
- Vil trusselen for tyveri av data minimeres.

Etabler verdi av data for backup.

Når det gjelder backup- og restore-løsninger, er det ikke samme standard for alle. Hva slags løsning dere velger bestemmes av verdien av dataene som skal beskyttes. Data som ikke er viktig trenger ingen dyr backup-løsning. Data som er livsnerven i bedriften din trenger den beste beskyttelsen du kan få tak i.

For å vurdere verdien av dataene dine:

1. Kategoriser først forretningsdataene du vil ta backup av – det viktige, det svært viktige og det helt avgjørende.
2. Spør deg selv “Hva er verdien av disse dataene for hver time de er utilgjengelige?
3. Hva er konsekvensene hvis disse dataene går tapt for alltid?
4. Hva er konsekvensene hvis det faller i gale hender?”

Ved å kategorisere dataene dine i henhold til verdien, vil du klare å lage en plan som passer best til kostnadene ved backup til kvaliteten av nødvendig beskyttelse. Så kan du etablere et system i henhold til følgende betraktninger for hver av de tre viktigste backup-teknologiene.

Backup-alternativer:
Lokal backup, cloud backup og hybrid cloud backup

For å hjelpe deg gjennom alle hensynene ved å velge system har vi laget en tabell som identifiserer styrke og svakheter ved de tre backup-alternativene.

Lokal backup: Dette er metoden for å sikkerhetskopiere en lokal tape eller disk som selskapet oppbevarer på stedet. Det er bra for rask gjenoppretting, men sårbart og tidkrevende ved behov for restore.

Cloud backup: Metoden for å lagre data eksternt. Cloud-løsninger bruker internett for å laste opp backupdata til et eksternt datasenter. De beste cloud løsningene automatiserer denne prosessen slik at brukeren

enkelt kan installere det. Det finnes to nivåer av backup-systemer i cloud: forbruker-løsninger og bedriftsløsninger. I motsetning til bedriftsløsningene, er forbruker-løsningene ofte svært rimelige (eller gratis), men tilbyr lite support, sikkerhet eller egnede SLA.

Hybrid cloud backup: Enkle cloud backup-løsninger har ett problem: I en datakrise der store mengder data må gjenopprettes fra cloud, er ofte overføringen via nettet for langsom. En hybrid cloud backup-løsning løser dette ved å legge til en integrert lokal backup til backupsystemet i cloud. Samme automatisering sikrer **enkel og rask installasjon**, og duplisert lokal backup betyr at data kan gjenopprettes i løpet av få minutter i stedet for timer.