

6 kritiske grunde til, hvorfor Office 365 backup er nødvendigt

Lær mere om, hvorfor og hvordan du selv
kan beskytte dine Office 365-data.



Har du selv styr på dine Office 365-data?

De fleste vil nok sige: Ja, det har jeg. Eller: Det har Microsoft. Og ja, Microsoft sørger ganske rigtigt for meget og tilbyder også sine kunder et fantastisk produkt i Office 365.

Dog skal du vide, at Microsoft først og fremmest sørger for, at der er styr på infrastrukturen, og at platformen er tilgængelig. Ansvar for de data, der ligger på platformen, er dit – og dit alene.

Det er en udpræget misforståelse, at Microsoft tager fuld backup af dine data. Det gør de ikke. Og jo før du bliver bevidst om det, jo bedre. I sidste ende er det nemlig din opgave at sikre, at du har adgang til – og kontrol over – de data, du har i Exchange Online, SharePoint Online, OneDrive for Business og Microsoft Teams.

I dette whitepaper kan du læse mere om, hvad der – i værste fald – kan ske, hvis ikke du tager backup af dine Office 365-data.



Den store Office 365- misforståelse

Misforståelsen bunder i, hvad brugeren mener er Microsofts ansvar (ift. beskyttelse og retention af Office 365-data), og hvad brugeren reelt set har ansvar for.

Vi ser også ofte, at der er forskel på, hvor meget backup og gendannelse Microsoft egentlig tilbyder, og det, som brugeren tror, han får.

Som eksempel tilbyder Microsoft Office 365 georedundans. Det misforstås ofte som backup. Backup sker dog kun, når der laves en historisk kopi af data, og når den gemmes på en anden lokation. Det er ikke tilfældet med georedundans. Det sikrer blot, at et andet datacenter tager over, hvis du og dine brugere ikke kan få adgang til Office 365 gennem det første.

For at have rigtig backup skal du have direkte adgang til – og kontrol over – dine data.

Har du det, vil du til gengæld hurtigt kunne gendanne dine data og arbejde videre, selv hvis dine data skulle forsvinde, blive slettet eller taget som gidsel af fx ransomware.





6 grunde til hvorfor Office 365 Backup er nødvendigt

Microsoft Office 365 er en fremragende Software-as-a-Service (SaaS)-platform, der fuldt ud opfylder de behov, som mange virksomheder har til en platform af denne type.

Med Office 365 får du høj opetid og høj tilgængelighed, der sikrer, at du og dine kolleger kan forblive produktive, men kun med Office 365 Backup får du fuld beskyttelse mod sikkerhedstrusler.

Måske tænker du, at den papirkurv, som Office 365 stiller til rådighed, er fin til dine gendannelsesbehov. Her tager du fejl. Det tager i gennemsnit 140 dage, fra dine data bliver kompromitteret, til det bliver opdaget. Det er stort spænd, og der er stor

sandsynlighed for, at du først opdager, at du mangler en fil, når den ikke længere kan gendannes fra papirkurven. Et studie, som den markedsledende backupleverandør Veeam har foretaget blandt flere hundrede virksomheder med Office 365, viser, at datatab typisk optræder i 6 scenarier:

1. Tilfældig sletning
2. Usikkerhed omkring regler og politikker
3. Interne sikkerhedstrusler
4. Eksterne sikkerhedstrusler
5. Lovkrav og compliance
6. Administration af hybride e-mailmiljøer



1. Tilfældig sletning

Sletter du en bruger, uanset om det er hensigten eller ej, sker det på tværs af netværket og sammen med sletning af brugerens personlige SharePoint-site og OneDrive-data. Office 365s indbyggede papirkurv og versionshistorik beskytter kun i begrænset grad mod datatab.

Det betyder, at selv en simpel gendannelse fra en ægte backup kan blive en stor udfordring, hvis data for altid er slettet på tværs af netværket, eller hvis tilbageholdelsesperioden er udløbet. På Office 365-plattformen kan du slette på to måder, soft delete og hard delete.

Et eksempel på en soft delete er, hvis du tømmer Deleted Items-mappen (DA: Slettede elementer). Denne type sletning kaldes også "Permanently deleted" – også selvom du stadig vil kunne finde slettede element i "Recoverable Items"-postkassen.

Straks værre er det med hard delete. Hard delete sker, når et element – som fx en vigtig mail - får et tag, der fjerner det helt fra postkassens database. Sker det, kan elementet ikke gendannes.

2. Usikkerhed omkring regler og politikker

Den digitale tidsalder byder hele tiden på nye forretningssmuligheder og regler og politikker, der er svære at holde sig opdateret på og administrere.

Ligesom tilfældet var med hard og soft delete, er Office 365s backup- og gendannelsesmuligheder begrænsede og hjælper kun i ringe grad mod datatab.

De kan derfor på ingen måde erstatte en ægte backupløsning, som i modsætning til Microsoft fx tilbyder point-in-time-gendannelse af elementerne i din postkasse.

Skulle uheldet være ude, kan du med en backupløsning lave en rollback til et helt bestemt tidspunkt, før uheldet skete. Du undgår også at bruge tid på at sætte dig ind i, hvad Microsoft (ikke) har og tager ansvar for. Med Office 365 Backup kan du lave backup, du kan bruge på kort sigt, eller gemme som arkivdata. Gendannelse er altid hurtigt, nemt og pålideligt.



3. Interne sikkerhedstrusler

Sikkerhedstrusler forbindes ofte med hackere eller virus, men det er i virkeligheden en anden slags trussel, virksomhederne oftest er truet af. Medarbejderne er nemlig virksomhedens største sikkerhedstrussel, og det gælder både overlagt sletning af data og data, der bliver slettet ved en fejl.

Adgange til kritiske data som fx filer og kontakter skifter så hurtigt, at det som virksomhed kan være svært at følge med i, hvem der har adgang til hvad. Microsoft har fx heller ikke mulighed for at vide, om medarbejderen er blevet opsagt, hvis han forsøger at slette kritiske virksomhedsdata, før han forlader virksomheden. Uden at vide det kan medarbejderne også udgøre en sikkerhedsfare ved at downloade inficerede filer og – ubevidst – udlevere brugernavne og passwords til hjemmesider, de troede, de kunne stole på.

Et andet eksempel på en intern sikkerhedstrussel er forfalskning af bevismateriale. Det kan fx være en medarbejder, der bevidst sletter belastende e-mails og filer for at undgå, at andre i organisationen får kendskab til dem.

4. Eksterne sikkerhedstrusler

Malware og virus – som fx ransomware – har gjort stor skade på virksomheder over hele verden. Rammer de dig, er det ikke kun din virksomheds omdømme, der bliver ramt.

Det gælder også den fortrolighed og sikkerhed, der bør og skal være omkring dine interne data og kundedata. Eksterne trusler kan snige sig ind i form af e-mails og vedhæftninger, og det er ikke altid nok at undervise medarbejderne i, hvad de skal holde øje med.

Angriberne bliver nemlig hele tiden bedre til at få de enkelte e-mails til at se mere overbevisende ud. Skulle du blive ramt af malware eller virus, tilbyder Exchange Online ikke den funktionalitet, du skal bruge for at gendanne dine data.

Kun med en dedikeret backupløsning sikrer du, at dine data ikke bliver inficeret, og at de hurtigt kan gendannes.



5. Lovkrav og compliance

Som en del af en juridisk proces – som fx et sagsanlæg – kan du risikere på et tidspunkt at skulle fremskaffe bestemte e-mails, filer eller andet data.

Skulle det ske for dig, har Microsoft et indbygget sikkerhedsnet (Litigation Hold). Dog tilbyder løsningen ikke den funktionalitet, du skal bruge for at være sikker på at undgå evt. bøder.

Sletter du fx en bruger ved en fejl, sletter du også hans indbakke, hans personlige SharePoint-site og hans OneDrive-konto. Det kan blive dyrt – og besværligt – at rode sig ud af.

Lovkrav, compliancereger og adgangsregulering varierer selvfølgelig på tværs af industrier og lande, men bøder, straffe og juridiske tvister pga. manglende adgang til dine data er i hvert fald tre ting, du ikke vil og bør bruge tid på.

6. Administration af hybride e-mailmiljøer

Virksomheder, der skifter til Office 365, har typisk brug for en midlertidig, hybrid løsning, hvor de har en del af deres Exchange-løsning lokalt (on-prem) og en anden i Office 365 Exchange Online.

At Exchange-data kan ligge både lokalt og i skyen, kan godt give visse udfordringer rent teknisk, hvis du skal gendanne dem - især hvis du ikke har en backupløsning. Har du Office 365 Backup, er det ikke et problem, da løsningen behandler Exchange-data ens, uanset hvor den ligger.

Med Office 365 Backup vil du også kunne gemme dine backupdata, hvor du har lyst – fx lokalt (on-prem) eller som object storage i skyen.



Hvor ofte optræder scenarierne?

Du burde ikke længere være i tvivl om, hvorfor du bør tage backup af dine Office 365-data. Og undrer du dig over, hvor ofte de 6 scenarier, vi har gennemgået, finder sted, er svaret desværre; alt for ofte.

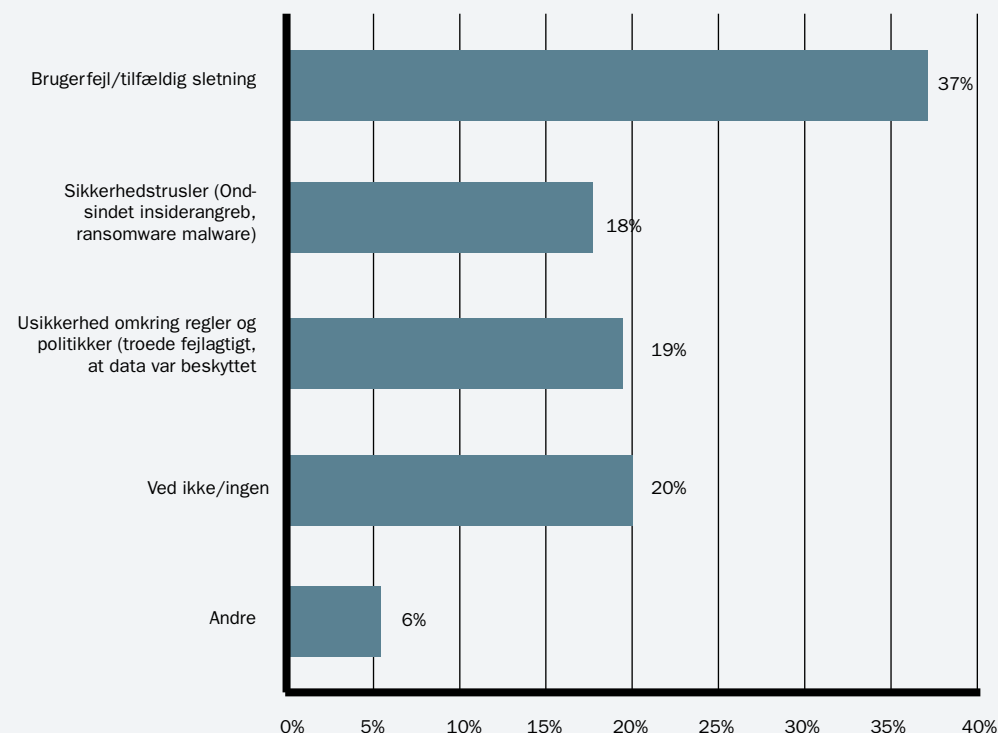
I undersøgelsen afbildet i grafen til højre blev mere end 1.000 it-medarbejdere spurgt om, hvilke former for datatab de har oplevet i skyen.

Hertil svarede mellem 18% og - helt op - til 37% af respondenterne, at de har oplevet datatab enten pga. brugerfejl/tilfældig sletning, sikkerhedstrusler eller usikkerhed omkring regler og politikker.

Til trods for det høje tal vurderer analysefirmaet IDC, at helt op til 76% af alle Office-dokumenter ikke har en backup. Faktisk vurderer de, at 6 ud af 10 virksomheder ikke har nogen som helst form for beskyttelse af Office 365-data.

Arbejder du i en virksomhed, der (heller) ikke tager backup? Hvis ja, har du forhåbentligt nu de argumenter, du skal bruge for at overbevise dine kolleger om vigtigheden af at tage backup af jeres Office 365-data.

Spørgsmål 14. Hvilke former for datatab har du oplevet i skyen? (Sæt kryds i alle, der gælder for dig)



Konklusion

Office 365 er, som vi tidligere har nævnt, et fremragende produkt, og har du læst med så langt, bruger din virksomhed højst sandsynligt allerede produktet. Office 365 er et fornuftigt valg, og det samme er en rigtig backupløsning, som giver dig:

- Fuld adgang til og fuld kontrol over dine Office 365-data
- Mulighed for at gendanne dine data, som de var, og hvor de lå
- Ro i maven, hvis uheldet skulle være ude

Vi håber, at du er blevet klogere på Office 365 Backup.

Har du spørgsmål til Office 365, Office 365 Backup, og hvilken værdi det giver dig og din virksomhed, er du meget velkommen til at kontakte os.

Du kan komme i gang fra helt ned til kr. 20,00 pr. md. Pr. bruger. Kontakt os på office365backup@aimit.dk eller +45 70 22 42 12.

