Case: Back-ups maken van Office 365

Belangrijke redenen voor organisaties om een back-up te maken van Office 365-data

CREMERS COMPUTER COMPANY

Inleiding

Heeft u controle over uw Office 365-data?
Heeft u toegang tot alle items die u nodig heeft?
Voorspelbare reacties zijn meestal: "Ja, natuurlijk"
of "Daar zorgt Microsoft wel voor".

Maar sta hier eens even bij stil. Weet u dat zeker?

Microsoft neemt u heel wat zorgen uit handen en is klanten fantastisch van dienst. Maar de belangrijkste focus van Microsoft ligt bij het beheer van uw Office 365-infrastructuur en het waarborgen van de uptime voor uw gebruikers. De verantwoordelijkheid voor uw data ligt bij ù. Een veelgehoorde misvatting is dat Microsoft namens u een volledige back-up van uw data maakt. Als die denkwijze niet verandert en deze verantwoordelijkheid niet wordt opgepakt, kunnen de gevolgen desastreus zijn.

Uiteindelijk is het aan u om ervoor te zorgen dat uw data toegankelijk zijn en dat u controle erover heeft.

In dit rapport wordt onderzocht wat de risico's zijn als een back-up van Office 365 in uw arsenaal ontbreekt. Ook wordt nagegaan waarom back-upoplossingen voor Microsoft Office 365 voorzien in langdurige retention en databeveiliging.

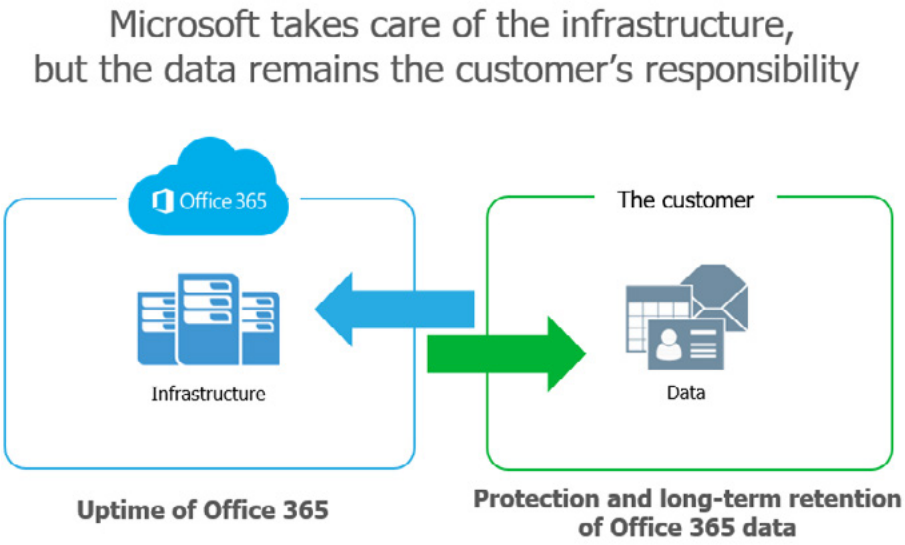
"We maakten ons zorgen over de beleidsregels voor back-up en retention in Office 365. Microsoft zorgt voor onze data, en het beveiligen van historische e-mailgegevens is belangrijk. Daarom hebben we besloten dat een back-up van onze data in Office 365 onontbeerlijk is."

— ***Karen St.Clair***, IT Manager,
Columbia Power & Water Systems

De grote misvatting over Office 365

Doorgaans wordt aangenomen dat Microsoft verantwoordelijk is voor de beveiliging en de langdurige retention van Office 365-data, terwijl die verantwoordelijkheid in werkelijkheid bij de gebruiker ligt. Daar ligt het misverstand. De back-up-en herstelmogelijkheden die Microsoft biedt verschillen vaak van wat gebruikers verwachten. Naast de standaardvoorzorgsmaatregelen van Office 365 moet u dus mogelijk nog eens moet nagaan in hoeverre u controle over uw data heeft en hoeveel toegang u er werkelijk toe heeft.

Microsoft Office 365 biedt geografische redundantie, wat vaak ten onrechte voor back-up wordt aangezien. Van een back-up is sprake wanneer er historische kopieën van data worden gemaakt en vervolgens op diverse locaties opgeslagen. Er is dan altijd een gemakkelijk toegankelijke kopie elders wanneer bijvoorbeeld data verloren gaan, per ongeluk worden verwijderd of door een kwaadwillige aanval beschadigd raken. Geografische redundantie biedt daarentegen bescherming bij locatieproblemen of hardwarestoringen. Bij een of andere crash van de infrastructuur of bij een storing blijven uw gebruikers Always-On en merken ze niet eens dat er problemen zijn.



"Met Office 365 zijn het ùw data. U bent eigenaar. U heeft er controle over."

— ***Microsoft***

6 redenen waarom het maken van back-ups van Office 365 zo belangrijk is

Als krachtig, optimaal presterend SaaS-platform (Software as a Service) voorziet Microsoft Office 365 perfect in de behoeften van veel organisaties. Office 365 zorgt voor beschikbaarheid van applicaties en uptime van systemen zodat uw gebruikers niets missen, maar een back-up van Office 365 kan u tegen veel andere praktijksituaties beschermen.

Uit gesprekken met honderden IT-professionals overal ter wereld die naar Office 365 zijn gemigreerd, blijkt dat er zes valkuilen overblijven met betrekking tot databeveiliging: per ongeluk wissen van data, hiaten in het retentionbeleid en verwarring daarover, interne beveiligingsrisico's, externe beveiligingsrisico's, wettelijke en compliancevereisten en het beheer van hybride e-mailimplementaties en migraties naar Office 365.

Elk commercieel bedrijf, groot én klein, moet nagaan of het IT-team alles onder controle heeft en of bedrijfskritische data altijd toegankelijk blijven.

Per ongeluk wissen

Hiaten in het retentionbeleid en verwarring daarover

Interne beveiligingsrisico's

Externe beveiligingsrisico's

Wettelijke en compliancevereisten

Beheer van hybride e-mailimplementaties en migraties naar Office 365

1
Per ongeluk wissen

Geografische redundantie vormt geen bescherming tegen iedere vorm van dataverlies. Als u bijvoorbeeld, al dan niet bedoeld, een gebruiker verwijdert wordt die actie in het hele netwerk gerepliceerd.

De native prullenbakken en versiegeschiedenis in Office 365 bieden slechts beperkte beveiliging tegen dataverlies. Een eenvoudige herstelactie kan een groot probleem worden zodra Office 365 de data via geografische redundantie voorgoed heeft verwijderd.

Op het Office 365-platform kunnen data op twee manieren worden verwijderd: voorlopig en permanent. Bij voorlopig verwijderen maakt u bijvoorbeeld de map Verwijderde items leeg. Dit wordt ook wel "Definitief verwijderd" genoemd. In dit geval is definitief niet echt definitief, want het item staat nog in het postvak Herstelbare items.

Bij permanent verwijderen wordt een item gemarkeerd voor volledige verwijdering uit de database met postvakken. Zodra dit gebeurt is het item voorgoed verdwenen, punt uit.

Tenzij er op de achtergrond een back-upoplossing actief is.

2
Hiaten in het retentionbeleid en verwarring daarover

In dit digitale tijdperk van snel zakendoen worden beleidsregels voortdurend bijgesteld, waaronder ook het retentionbeleid, wat moeilijk bij te houden is, laat staan te beheren. Net als bij permanent en voorlopig verwijderen, beschikt Office 365 maar in beperkte mate over beleidsregels voor back-up en retention. Deze kunnen slechts situationeel dataverlies voorkomen en zijn niet bedoeld als alles omvattende back-upoplossing.

Van medewerkers die bijvoorbeeld uit dienst gaan, worden de gegevens door Microsoft maar 90 dagen bewaard, afhankelijk van de specifieke instellingen. Microsoft is alleen belast met handhaving van het retentionbeleid zoals in de serviceovereenkomst vermeld; al het andere zou als contractbreuk kunnen worden beschouwd. Het maken van back-ups van gegevens van ex-medewerkers is essentieel. IT-beheerders vergissen zich vaak in de aanwezige dekkingsgraad totdat die belangrijke gegevens verdwenen zijn.

Met een back-upoplossing voor Office 365 kan een uitgebreider, toegankelijker retentionbeleid verkregen worden waarmee al uw data beveiligd en op één locatie opgeslagen worden, waardoor herstel snel, eenvoudig en betrouwbaar wordt.

3 Interne beveiligingsrisico's

Bij een beveiligingsrisico denken we al snel aan hackers en virussen. Bedrijven hebben echter te maken met risico's met een interne oorzaak, en dat gebeurt vaker dan u denkt. Organisaties worden het slachtoffer van risico's die door hun eigen medewerkers zowel met opzet als per ongeluk worden veroorzaakt.

Toegang tot bestanden en contactpersonen verandert zo snel dat het lastig kan zijn om te letten op de mensen die u het meest vertrouwt. In Microsoft is het onmogelijk een gewone gebruiker te onderscheiden van een ex-medewerker die vóór vertrek probeert om cruciale bedrijfsgegevens te verwijderen. Bovendien zorgen sommige gebruikers onbewust voor ernstige risico's door geïnfecteerde bestanden te downloaden en per ongeluk gebruikersnamen en wachtwoorden kenbaar te maken aan sites die betrouwbaar leken. Er is een zekere mate van training nodig om deze kwesties het hoofd te bieden, maar menselijke fouten en kwade bedoelingen zullen altijd een bedreiging vormen als er geen adequate beveiligingsmaatregelen zijn genomen, zoals het maken van back-ups.

4 Externe beveiligingsrisico's

Malware en virussen, zoals ransomware, hebben het afgelopen jaar over de hele wereld ernstige schade aan organisaties toegebracht. Niet alleen staat de reputatie van een bedrijf op het spel, maar ook de privacy van interne en klantgegevens. Beperking van reputatieschade na een inbreuk is niet eenvoudig. Externe risico's sluipen binnen via e-mailberichten en bijlagen, en het is niet altijd voldoende om gebruikers te leren waarop ze moeten letten, vooral wanneer de geïnfecteerde berichten zo aantrekkelijk lijken. De functies van Exchange Online voor back-up en herstel zijn onvoldoende om ernstige aanvallen op te vangen. Regelmatige back-ups helpen voorkomen dat een externe aanval uit de hand loopt.

5
Wettelijke en compliancevereisten

Soms moet u onverwacht postvakken of andere typen data ophalen met het oog op een juridische procedure. U denkt dat iets onmogelijk kan gebeuren, totdat het gebeurt. Microsoft biedt een aantal vangnetten (instellingen zoals In-place bewaring en Bewaren van postvakgegevens vanwege juridische procedure), maar ook hiervoor geldt dat deze geen solide back-upoplossing vormen waarmee uw bedrijf uit de juridische problemen wordt gehouden. Als u bijvoorbeeld per ongeluk een gebruiker verwijdert, wordt ook zijn of haar on-hold postvak verwijderd.

Wettelijke vereisten, compliancevereisten en toegangsregelgeving zijn in elke branche en in elk land anders, maar boetes, strafrechtelijke vervolging en juridische geschillen zijn drie dingen die u liever niet op uw actielijstje ziet.

6
Beheer van hybride e-mailimplementaties en migraties naar Office 365

Organisaties die voor Office 365 kiezen hebben meestal tijd nodig voor de transitie van on-premises Exchange naar Office 365 Exchange Online. Sommige bedrijven houden zelfs een klein deel van het traditionele systeem in stand voor extra flexibiliteit en aanvullende controle. Deze hybride e-mailimplementaties komen vaak voor, maar maken het beheer ook extra uitdagend. De juiste back-uplossing voor Office 365 moet geschikt zijn voor hybride e-mailimplementaties en moet Exchange-data, ongeacht de bronlocatie ervan, precies hetzelfde afhandelen.

Conclusie

Wij nodigen u uit om op onderzoek uit te gaan. Mogelijk is er sprake van een hiaat waarvan u zich niet bewust bent.

U heeft al een verstandig zakelijk besluit genomen door Microsoft Office 365 te implementeren. Ga nu — om onnodige risico's van dataverlies te voorkomen — op zoek naar een back-up oplossing die u zowel volledige toegang tot uw Office 365-data als volledige controle over deze data biedt.

Lees meer over Office 365-back-up:
https://www.c3ict.nl/online-backup-office365


CREMERS
COMPUTER
COMPANY