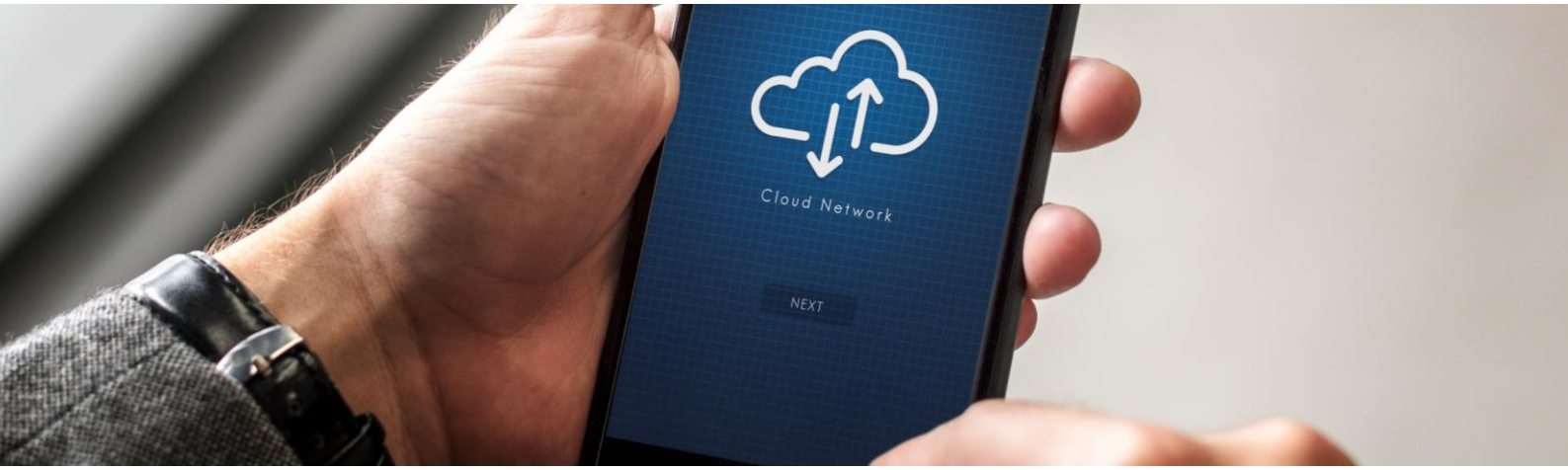
ilionx
Your partner in digital business



Nooit meer dataverlies door snelle Cloud back-up Microsoft 365

Veel gebruikers hebben de beleving dat alle data die ze in de Cloud plaatsen per definitie veilig is. Een van de diensten waar dit voor geldt is Office 365. In de praktijk blijken hier echter nogal wat haken en ogen aan te zitten.

Backups, recycle bin and versioning

Office 365 kent in totaal een 4-tal methodes om data veilig te stellen:

1. De backup die Microsoft zelf maakt;
2. Het Recycle bin proces;
3. Retentie;
4. Versioning.

1. Backups

Microsoft heeft het backup proces primair ingeregeld om zelf te kunnen gebruiken in geval van een calamiteit. Microsoft geeft aan elke 12 uur een backup te maken en een retentie periode aan te houden van 14 dagen.

Zoals aangegeven is de backup ingeregeld voor disaster recovery doeleinden en hierdoor is het alleen mogelijk om complete omgevingen te kunnen terugzetten. Het is dan ook niet mogelijk om zogenaamde bricklevel restores te kunnen uitvoeren van bijvoorbeeld een individuele mailbox of een mailbox item.

Restores moeten worden aangevraagd via de support-afdeling van Microsoft. Nadeel hiervan is dat je geen controle hebt over het moment waarop de restore daadwerkelijk wordt uitgevoerd. Verder zijn er kosten verbonden aan deze restores.

2. Recycle bin proces

Wanneer data wordt weggegooid wordt deze opgeslagen in de recycle bin. Naast de standaard recycle bin kent Office 365 zowel voor mail als voor Sharepoint nog een tweede recycle bin waar de data wordt opgeslagen wanneer deze uit de primaire recycle bin wordt verwijderd.

Alhoewel het idee bij zowel mail als Sharepoint hetzelfde is, is er toch een verschil in de exacte werking. Om die reden hebben we het proces van beide hieronder kort beschreven.

Mail

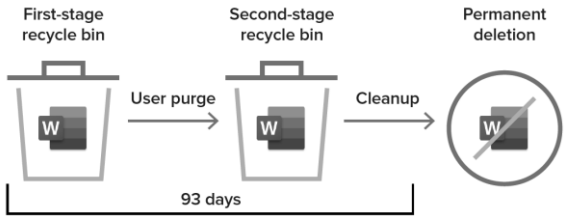
Het proces voor mail ziet er als volgt uit:

1. De gebruiker verwijdert data;
2. Het item wordt opgeslagen in de ‘deleted items’ folder. In principe kan een item daar voor een onbepaalde tijd blijven staan;
3. Wanneer data wordt verwijderd uit ‘deleted items’ wordt deze naar de 2e recycle bin ofwel de

'recoverable items' verplaatst. Hier blijft de data maximaal 30 dagen in staan;
4. Na 30 dagen wordt de data definitief verwijderd.

Sharepoint

Bij Sharepoint ziet het proces er als volgt uit:
1. De gebruiker verwijdert data;
2. De data wordt verplaatst naar de 'First-stage recycle bin', ook wel de 'Site recycle bin' genoemd;
3. Wanneer de data verwijderd wordt uit de 'First-stage recycle bin' wordt deze verplaatst naar de 'Second-stage recycle bin' welke ook wel 'Site collection recycle bin' genoemd wordt;
4. In alle gevallen wordt de data permanent verwijderd na 93 dagen nadat de data voor het eerst in de 'First-stage recycle bin' geplaatst is. Het maak hierbij niet uit in welke recycle bin de data op dat moment staat. Verwijderde data wordt binnen Sharepoint dus voor maar maximaal 93 dagen bewaard.

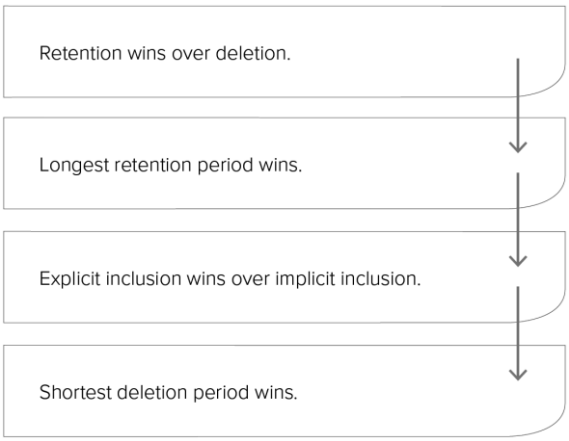


3. Retentie

Binnen de Office 365 abonnementen E3, E5 en Exchange online is het mogelijk om gebruik te maken van retentie. Microsoft heeft retentie geïntroduceerd om een tweetal redenen:
• Data voor een bepaalde periode bewaren;
• Data na een bepaalde periode verwijderen.

Aangezien deze elementen strijdig aan elkaar kunnen zijn gelden een aantal regels met betrekking tot retentie:

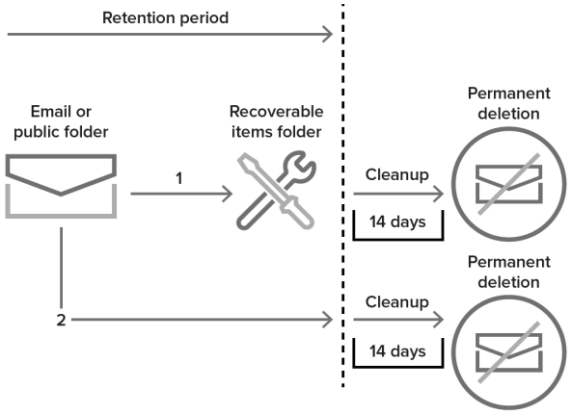
The principles of retention



Ook bij retentie is er een verschil in de werking tussen mail en Sharepoint. Hieronder zijn deze los beschreven:

Mail

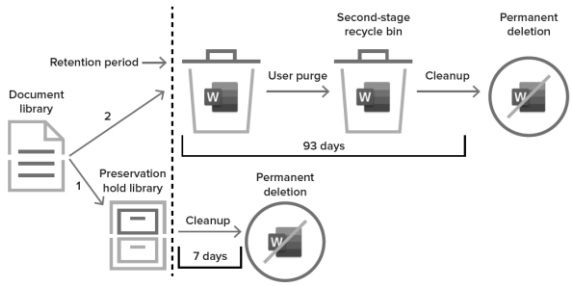
Het retentieproces voor mail ziet er als volgt uit:
• Items worden bij het verwijderen uit de 'deleted items' folder verplaatst naar de 'recoverable items' folder;
• Periodiek draait er een proces welke controleert of items voldoen aan de ingestelde retentie policy. Als dit niet het geval is worden items definitief verwijderd. Als dit wel het geval is blijven de items in de 'recoverable items' folder staan.



Sharepoint

Zoals aangegeven is het retentieproces in Sharepoint anders en afhankelijk of de data al bestaat op het moment dat de retentie policy wordt aangemaakt.

Op het moment dat de data al bestaat bij het aanmaken van de retentiepolicy wordt er een versie van de data weggeschreven op een van de volgende momenten:
• Op het moment dat de eerste wijziging wordt doorgevoerd in het document nadat de retentie policy is aangemaakt. De versie van voor de wijziging wordt weggeschreven naar de 'Preservation Hold Library';
• Op het moment dat de data wordt verwijderd.



Het is belangrijk om te realiseren dat retentie maar 1 versie oplevert van de data. Wanneer je meerdere versies van een bestand wil bewaren, dien je gebruik te maken van versioning.

4. Versioning

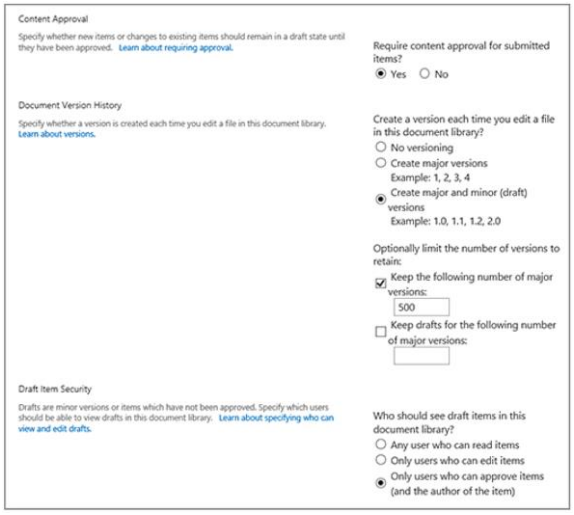
Wanneer versioning is geactiveerd worden verschillende versies van de data opgeslagen. Net als bij retentie is er ook hier een verschil in de werking tussen mail en Sharepoint. Beide worden hieronder dan ook los behandeld.

Sharepoint

Bij Sharepoint kan versioning los van retention worden geactiveerd. Ook bij abonnementen waar geen gebruik gemaakt kan worden van retention, kan versioning worden geactiveerd.

Versioning is voor Sharepoint dan ook niet alleen beperkt tot E3 en E5 abonnementen.

In onderstaand screenshot is terug te vinden welke instellingsmogelijkheden er zijn voor versioning binnen Sharepoint.



Mail

In tegenstelling tot Sharepoint is bij mail de mogelijkheid van versioning wel gekoppeld aan retention. Versioning voor mail is dan ook alleen beschikbaar voor mensen die gebruik van maken van een E3, E5 of Exchange Online 2 abonnement.

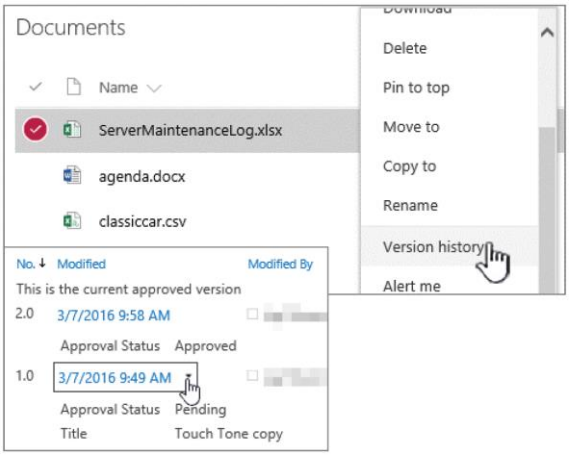
Zodra retention is geactiveerd worden er automatisch versies van een mail item opgeslagen in de volgende situaties:
• Subject van een mailbox item wijzigt;
• Body van een mailbox item wijzigt;
• Er wordt een attachment aan een mailbox item toegevoegd of van een mailbox item verwijderd;
• Er worden verzenders of ontvangers toegevoegd aan een mailbox item;
• De verzonden of ontvangen datum van een mailbox item wordt gewijzigd.

Restore proces

Het belangrijkste onderdeel van een backup is de restore en het restore proces. Hieronder hebben we beschreven hoe dit proces eruit ziet voor zowel Sharepoint als mail.

Sharepoint

Binnen Sharepoint is het alleen mogelijk om versies per file terug te zetten. Het proces ziet er als volgt uit:
1. Selecteer de file;
2. Druk op de rechtermuisknop en kies voor ‘version history’;
3. Selecteer de gewenste datum en kies voor ‘restore’.



Zoals gezegd is het met de standaard tools binnen Sharepoint niet mogelijk om bestanden in bulk te kunnen terugzetten. Dit betekent ook dat het met de standaard tools niet goed mogelijk is om te recoveren van een ransomware aanval.

Mail

Voor mail ziet het recovery proces er globaal als volgt uit:
1. Maak een nieuw filter aan binnen ‘In-place eDiscovery & hold’ wat zich bevindt in de sectie ‘compliance management’;
2. Exporteer de items die voldoen aan het filter naar een .PST file;
3. Open de .PST file in Outlook. De items worden binnen een nieuwe map in Outlook geplaatst;
4. Sleep de gewenste items uit de nieuwe map naar de gewenste map in Outlook.

Het is belangrijk om aan te geven dat het niet mogelijk is om een zogenaamde point in time restore uit te voeren voor mail.

Redenen om te kiezen voor een 3rd-party backup oplossing

Alhoewel er binnen Office 365 mogelijkheden zijn om data terug te kunnen halen, kunnen we constateren dat de genoemde mogelijkheden niet afdoende zijn om data in elke situatie veilig te kunnen stellen.

Hieronder een overzicht van de belangrijkste redenen om een 3rd party backup tool in te zetten om de data binnen Office 365 optimaal te kunnen beschermen:

1. Mogelijkheid om de data vendor onafhankelijk veilig te stellen:
- Ook toegang tot de data bij problemen bij Microsoft;
- Ook data kunnen herstellen in geval van bijvoorbeeld corruptie van een mailbox of een site;
- Voor veel organisaties is dit een vereiste op basis van wet- en regelgeving.

2. Standaard retentie is beperkt:
- Voor e-mail slechts 30 dagen;
- Voor Sharepoint slechts 90 dagen;

3. Wanneer langere retentie gewenst is, kan binnen Office 365 gekozen worden voor een E3 of E5 abonnement in plaats van Business Premium. Echter de kosten voor een Business Premium abonnement en een 3rd- party backup tool samen liggen beduidend lager dan de kosten van een E3 of een E5 abonnement;

4. Office 365 biedt geen bulk point-in-time restore mogelijkheid en biedt dus standaard ook geen mogelijkheid om te kunnen recoveren van ransomware.
- Bij e-mail kan alleen een datum selectie gemaakt worden op basis van de datum waarop de e-mail is gecreëerd;
- Bij Sharepoint kan alleen per file een restore worden uitgevoerd.

5. Lage en gegarandeerde RTO. Binnen Office 365 wordt veelal gebruik gemaakt van tools die niet primair ontwikkeld zijn voor backup- en restore

doeleinden. Hierdoor kan het soms omslachtig en tijdrovend zijn om de tools te gebruiken, wat de RTO niet ten goede komt;

6. Een 3rd-party backup tool biedt de mogelijkheid om rapportages te genereren van het backup proces. Op die manier kan worden gecontroleerd of de backup goed functioneert. Office 365 biedt hiervoor geen mogelijkheden;

7. Zoals eerder aangegeven gebruikt Office 365 tools voor de backup die niet primair ontwikkeld zijn voor backup & restore doeleinden. Hierdoor kan er onduidelijkheid ontstaan over wat er nu wel en niet geregeld is en is het lastig om klanten de garanties te geven die ze verwachten;

8. Ransomware, CEO fraude, Account Compromise voorkomen. Hierbij proberen kwaadwillenden met social engineering je gebruikers te verleiden tot het afgeven van de inloggegevens van jouw Office 365 omgeving. Om vervolgens die accounts te mailen en anderen te bewegen data te delen of bedragen over te maken.

Wij zien dit in de praktijk steeds vaker gebeuren. Criminelen verdienen steeds meer geld aan CEO-fraude, zoals blijkt uit een reportage die de NOS hierover heeft gemaakt:

- https://nos.nl/artikel/2250066-criminelen-verdienen-steedsmeer-geld- aan-ceo-fraude.html

Is Office 365 veilig? De opvatting heerst dat deze omgeving volledig beveiligd is en onder verantwoording valt van Microsoft. Hoeveel risico loop je dus als organisatie?

Met een scan die we samen met partner Barracuda hebben ontwikkeld, brengen we dit in kaart. We onderzoeken de risico's van business e-mail compromises, phishing pogingen, domein fraude, basic anti-fraudetraining en cyberfraude.

Lees ook onderstaande links:

- https://latesthackingnews.com/2018/08/17/new-hacking-technique-used-to-bypass-microsoft-office-365s-security/
- https://thehackernews.com/2018/05/microsoft-safelinks-phishing.html

9. 3rd-party backup tools zijn over het algemeen veel eenvoudiger in gebruik dan de tools die standaard beschikbaar zijn binnen Office 365.

Wil je hier meer over weten?

Neem dan vrijblijvend contact op met **Freek van Dieren** via 06 24 34 93 39 of fvandieren@ilionx.com

Over de auteurs

Deze whitepaper is tot stand gekomen in samenwerking met onze partner **Barracuda Networks** • barracuda.com