

SPECTRUM

A circular seal with the text "Unabhängiger KANZLEI Systempartner" around the perimeter, partially overlapping the "S" in the SPECTRUM logo.

Es wird Zeit für

SPECTRUM-Backup für M365

Wie sichern Sie heute
Ihre Daten aus



Microsoft 365 ?



Aus Exchange-Online ?



Aus MS-Teams ?



Aus OneDrive ?

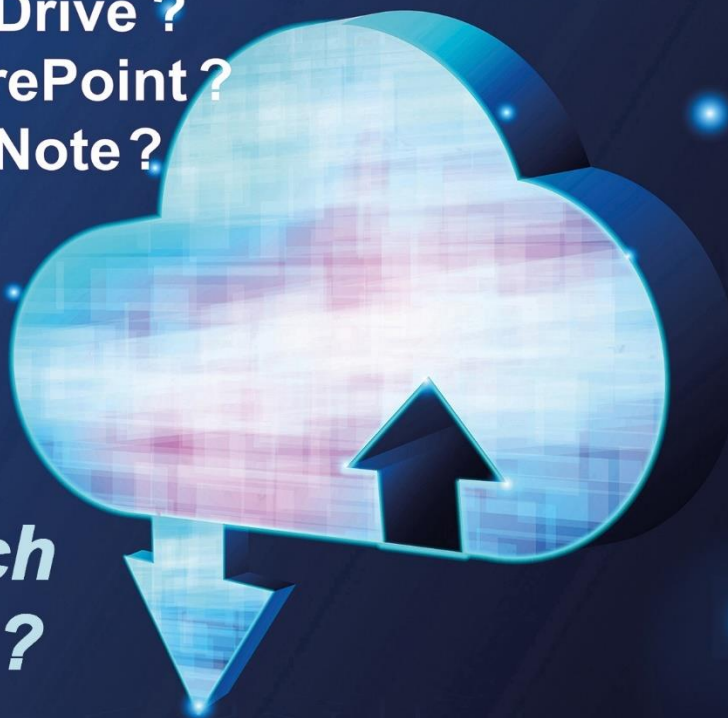


Aus SharePoint ?



Aus OneNote ?

*Etwa noch
garnicht ?*



Die IT wird immer komplexer:

Vor Jahren hatte man noch MS-Office mit Word, Excel, PowerPoint und Outlook ggfs. in Kombination mit einem Exchange-Server auf dem eigenen lokalen WTS-Server oder auf dem eigenen ASP-System installiert und genutzt. Die erstellten Daten und erhaltenen E-Mails wurden dabei auf dem eigenen Server abgelegt und mit der Server-Datensicherung einfach mitgespeichert – *im SPECTRUM-ASP-System mit einer doppelten Datensicherung sogar für bis zu 10 Jahre.*

Die Microsoft-365-Produkte werden heute immer populärer und viele Kunden haben auf Microsoft-365 (M365) gewechselt – *hierbei wird aber oft die Sicherung vergessen, da sich bei Microsoft-365 einige Daten nicht mehr auf dem eigenen Server oder dem eigenen ASP-System befinden – **die Microsoft-365-Daten liegen ohne Datensicherung einfach ungesichert in der Microsoft-Cloud.***

Die Verfügbarkeitszusagen von Microsoft:

Unter der Rubrik „Häufig gestellte Fragen zu Microsoft-365 für Unternehmen“ erklärt Microsoft die zugesicherte Zuverlässigkeit von Microsoft-365:

„Alle Microsoft-365-Dienste werden mit einer sehr hohen Verfügbarkeit von 99,9 Prozent angeboten“ – so die Microsoft-Aussage.

Hinweis: Microsoft übernimmt bei dieser Verfügbarkeitszusage für den reinen Infrastruktur-Betrieb aber einerseits keinerlei Haftung oder Schadensersatz-Zusagen und andererseits vor allem keinerlei Datensicherung!

Eine zugesicherte Verfügbarkeit von 99,9% bedeutet bei 24 Stunden pro Tag eine mögliche 0,1%ige Ausfallzeit, d.h. von nur 1,44 Minuten pro Tag – dies sind aber 8,76 Stunden pro Jahr! Die können ggfs. aber sehr wichtig sein!

Hinweis: Unter „Dienststatus“ werden der aktuelle Status des jeweiligen M365-Dienstes sowie Details zu Dienstunterbrechungen und -ausfällen von Microsoft im Internet angezeigt.

Dies sind z.B. die M365-Ist-Verfügbarkeitsangaben von Microsoft der letzten Jahre:

Jahr	Q1	Q2	Q3	Q4
2023	99,98%	99,99 %	99,99 %	99,996%
2022	99,98%	99,98%	99,99 %	99,99 %
2021	99,97%	99,98%	99,99 %	99,98%
2020	99,98%	99,99 %	99,97%	99,97%
2019	99,97%	99,97%	99,98%	99,98%

<https://learn.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity>

Wichtig: Diese Verfügbarkeitsangabe betrifft lediglich die Verfügbarkeit für die Bereitstellung der Infrastruktur von Microsoft bezüglich der Online-Dienste von Microsoft-365.

Die Verantwortung für die Daten generell und die Datensicherung obliegen alleine dem Kunden – ein Backup über mehrere Tage, Wochen oder Jahre ist generell nicht Bestandteil der Microsoft-365-Dienste und muss vom Anwender selbst organisiert werden!

Anwender verwechseln bei Microsoft-365 oft eine 99,9% „Funktions-Verfügbarkeit der Infrastruktur“ mit einer „Daten-Verfügbarkeit“ – dies ist aber leider falsch, weil Microsoft keine Datensicherung durchführt!

Microsoft stellt Kunden mit Microsoft-365 eine Vielzahl von Funktionen und Services zur Verfügung. Der Schwerpunkt liegt dabei jedoch ausschließlich auf dem Management der Microsoft-365-Infrastruktur und deren Verfügbarkeit für den Anwender.

Die Verantwortung für die Daten obliegt aber bei Microsoft-365 weiterhin ausschließlich dem Anwender!

Viele Kanzleien und Unternehmen gehen leider irrtümlich davon aus, dass ihre Daten in der Microsoft-Cloud auch vollständig gesichert werden - ***dies ist aber nicht der Fall!***

Dieser Irrglaube kann verheerende Folgen haben!

Jeder Anwender muss selbst sicherstellen, dass er seine Microsoft-365-Daten - *die in der Microsoft-Cloud liegen* – zusätzlich sichert:



d.h. die MS-Outlook/Exchange-Online-Daten

d.h. die MS-Teams-Daten

d.h. die MS-OneNote-Daten

d.h. die MS-OneDrive-Daten

d.h. die MS-SharePoint-Daten

Die Daten-Kontrolle ist bei Microsoft-365 Sache des Anwenders - wozu vor allem der Zugriffsschutz und die Datensicherung gehören.

Zur Datensicherung von Microsoft-365 gibt es das SPECTRUM-Zusatz-Produkt:

SPECTRUM-Backup für M365

Kurzspezifikation von „SPECTRUM-Backup für M365“:

Tägliche Nacht-Sicherung aller Daten aus den Microsoft-365-Anwendungen – d.h. aus MS-Outlook/Exchange-Online, aus MS-Teams, aus MS-OneNote, aus MS-OneDrive und aus MS-SharePoint-Online (Inkremental-Sicherung).

Die M365-Daten werden 10 Jahre gesichert:

Die Daten werden mit einem nachlaufenden „Sicherungs-Schweif“ für die Zeit von 10 Jahren verschlüsselt auf einem skalierbaren, webbasierten S3-Storage-Speicher in einem Cloud-Rechenzentrum in Deutschland gesichert.

Mit „SPECTRUM-Backup für M365“ stellen Sie sicher, dass Sie immer eine aktuelle Kopie Ihrer Daten haben, auf die Sie für 10 Jahre zurückgreifen und die Sie bei Bedarf wieder einspielen können.

Hinweis: Die Daten aus MS-Word, MS-Excel und MS-PowerPoint, die Sie lokal auf Ihrem Server oder ASP-System ablegen (z.B. in der DATEV-Dokumentenverwaltung oder in DATEV-DMS), werden natürlich weiterhin mit Ihrem bestehenden Datensicherungs-System gesichert.

Fünf Gründe warum ein Backup Ihrer Microsoft-365-Daten wichtig ist:



Löschen / Versehentliche Löschung

Wenn jemand einen Benutzer löscht (möglicherweise versehentlich), gilt diese Löschung im gesamten Netzwerk: Auch das „OneDrive for Business-Konto“ und sein „Outlook/Exchange“-Postfach in der Microsoft-Cloud, d.h. in Microsoft-365 werden gelöscht.

Die nativen Papierkörbe und Versionshistorien in Microsoft-365 bieten nur einen zeitlich eingeschränkten Schutz vor Datenverlust. So kann aus der Notwendigkeit einer einfachen Daten-Wiederherstellung schnell ein großes Problem werden, wenn Microsoft-365 die Daten unwiderruflich an allen Standorten gelöscht hat oder der kurze Aufbewahrungszeitraum des nativen Papierkorbes überschritten wurde.

Beispiel: Irgendjemand verlässt die Kanzlei, das Unternehmen und „räumt seinen Schreibtisch“ auf. D.h. er entfernt seine persönlichen Sachen aus den Schubladen und Schränken und löscht „sein“ Outlook-Postfach. Zunächst bemerkt dies keiner oder die Relevanz ist nicht sofort bewusst. Erst Monate später, wenn z.B. ein Konflikt bei einem Kunden oder Mandanten entstanden ist, fällt auf, dass in diesem persönlichen Postfach auch geschäftlich relevante E-Mails abgelegt waren, die jetzt nicht mehr vorhanden sind.

SPECTRUM kann hier aus der Erfahrung berichten, dass wir mehrfach pro Jahr in der Vergangenheit Exchange-Postfächer unserer Kunden zurücksichern mussten, da für wichtige Geschäftsvorfälle alte E-Mails wiederhergestellt werden mussten.



Interne Sicherheitsbedrohungen

Mit dem Begriff „Sicherheitsbedrohung“ werden meist Hacker-Angriffe und Viren assoziiert. Dabei sind Unternehmen auch Gefahren von innen ausgesetzt - und das häufiger als man denkt. Mitarbeiter können durch vorsätzliches oder unbeabsichtigtes Verhalten eine Bedrohung darstellen.

Der Zugriff auf Dateien und Kontakte ändert sich so schnell, dass es schwierig ist, die Personen im Blick zu behalten, denen Sie das größte Vertrauen entgegenbringen. Microsoft-365 bietet keine Möglichkeit, zwischen einem normalen Anwender und einem Mitarbeiter zu unterscheiden, der entlassen wurde und z.B. aus Frust versucht, wichtige Unternehmensdaten zu löschen. Manche Anwender gefährden zudem das Unternehmen, ohne es zu wissen, indem sie infizierte Dateien herunterladen und dann den eigenen Datenbestand verseuchen oder versehentlich Benutzernamen und Kennwörter auf vermeintlich vertrauenswürdige Hacker-Websites eingeben.



Ein weiteres Beispiel ist das Manipulieren von Beweisen, etwa wenn ein Mitarbeiter gezielt belastende E-Mails oder Dateien löscht, damit diese nicht von der Rechts-, Compliance- oder Personalabteilung gegen ihn verwendet werden können.

Beispiel: MS-Teams wird in Kanzleien und Unternehmen immer häufiger genutzt, um die interne Kommunikation zu organisieren. Für Projekte, Aufgabenstellungen oder Arbeitsgruppen laufen heute Kommunikationswege sehr oft in MS-Teams – inkl. aller Projektdokumentationen, Protokolle, Meetingverläufe, Meinungsbildungen usw.. Ist ein Projekt abgeschlossen, kümmert sich fast niemand mehr um diese Daten. Es gibt dann manchmal Leute auf allen Hierarchieebenen, die, um vermeintlich ggfs. Speicherplatz zu sparen, der Übersichtlichkeit Willen oder warum auch immer, komplette MS-Teams-Projekte einfach löschen – „Projekt ist ja abgeschlossen“ lautet oft die Begründung. Kommt es dann aber ggfs. zu einem Rechtsstreit, einer Auseinandersetzung mit dem Kunden bzw. Mandanten oder werden Vorgänge bei einer Betriebsprüfung hinterfragt usw. wird oft der Wunsch nach einer Datensicherung aus einem Backup gefordert.

3

Externe Sicherheitsbedrohungen / Cyberangriffe

Malware und Viren, wie z.B. Ransomware, haben Unternehmen schon weltweit großen Schaden zugefügt. Sie gefährden nicht nur das Ansehen eines Unternehmens, sondern auch den Schutz und die Sicherheit von internen Daten und Kundendaten.

Diese externen Bedrohungen werden durch E-Mails und Anhänge in Unternehmen eingeschleust. Nicht immer reicht es aus, die Anwender für die Gefahren zu sensibilisieren - insbesondere dann, wenn infizierte Nachrichten täuschend echt wirken. Die eingeschränkten Sicherungs- und Wiederherstellungsfunktionen z.B. von Exchange-Online, OneNote, OneDrive, SharePoint usw. bieten keinen ausreichenden Schutz vor schwerwiegenden Angriffen. Durch regelmäßige Backups können Sie sicherstellen, dass eine separate, nicht infizierte Kopie Ihrer Daten zur Verfügung steht, die eine schnelle Wiederherstellung ermöglicht.

4

Gesetzesvorschriften und Compliance-Anforderungen

Im Zuge von Rechtsverfahren müssen mitunter E-Mails, Dateien oder andere Datentypen abgerufen werden. Diese Situation tritt meist völlig unerwartet ein. Microsoft hat Microsoft-365 mit einigen Sicherheitsfunktionen versehen, doch diese stellen keine Backup-Lösung dar, mit der Ihr Unternehmen in einem Gerichtsverfahren alle erforderlichen Nachweise erbringen kann. Wenn Sie beispielsweise vor der Implementierung der gesetzlichen Aufbewahrung E-Mails oder Dokumente versehentlich löschen, sind Sie nur mit einer Backup-Lösung in der Lage, diese wiederherzustellen und Ihren gesetzlichen Pflichten nachzukommen.

Die Gesetzesvorschriften, Compliance-Anforderungen und Zugriffsregelungen sind von Branche zu Branche und von Land zu Land unterschiedlich. Bußgelder, Strafen und Rechtsstreitigkeiten gilt es jedoch in jedem Fall zu vermeiden. Auch die gesetzlichen Vorschriften für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte müssen hier berücksichtigt werden.



Beobachtungen zeigen, dass die Zahl der Nutzer, die MS-Teams-Umgebungen für Projekte und Initiativen einrichten, stetig steigt. Nach Abschluss eines Projekts benötigen Sie sehr wahrscheinlich eine Kopie der Projektdateien, um gesetzliche Aufbewahrungsvorschriften und Compliance-Vorgaben zu erfüllen.

Sehr häufig werden jedoch diese MS-Teams-Daten unbewusst/versehentlich gelöscht oder nicht den Vorschriften entsprechend aufbewahrt, sodass der Zugriff auf wichtige Dateien und Dokumente nicht mehr möglich ist.

5

Datenstrukturen in MS-Teams

Durch die Corona-Pandemie und die Umstellung auf das Arbeiten im Homeoffice hat sich die Zahl der Nutzer von MS-Teams innerhalb kürzester Zeit vervielfacht. MS-Teams wird nun in zahlreichen Unternehmen zentral eingesetzt, um die Produktivität zu steigern.

Die Anwendung besteht aus einer Benutzeroberfläche, über die Microsoft-365-Dienste wie SharePoint-Online und OneDrive for Business intransparent als Dateiablagen bereitgestellt und genutzt werden. Allerdings ist es für viele Anwender unübersichtlich, was wie und wo abgelegt wird. Ein M365-Backup stellt erst sicher, dass Sie auf alle Kopien Ihrer Daten zugreifen können, falls Originale versehentlich überschrieben werden oder verloren gehen.

Funktionsbeschreibung der Datensicherung SPECTRUM-Backup für M365

Funktionsübersicht

„**SPECTRUM-Backup für Microsoft 365**“ verhindert das Risiko von Datenverlust in Ihren Microsoft-365-Anwendungen, indem es eine umfassende Backup- und Wiederherstellungslösung bietet, die einfach zu implementieren und zu verwalten ist.

Als Backups werden regelmäßige Sicherungskopien bezeichnet, die im Rahmen einer Datensicherungsstrategie abgespeichert werden. Kommt es zu einem Datenverlust (z.B. durch Manipulation, Sabotage, Irrtum oder technischen Defekt), können so die jeweils aktuellen oder zeitlich aus der Vergangenheit benötigten Daten aus der Backup-Reihe wiederhergestellt werden (Restore).

Die kontinuierliche Datensicherung und das laufende automatische Monitoring bzw. die Überwachung der Datensicherungen gehören mit zu den wichtigsten Dienstleistungen im „SPECTRUM-Backup für M365“. Ihre Daten aus MS-Outlook/Exchange-Online, MS-Teams (einschließlich Kanäle und Registerkarten), MS-OneNote, MS-OneDrive und MS-SharePoint-Online werden täglich gesichert.

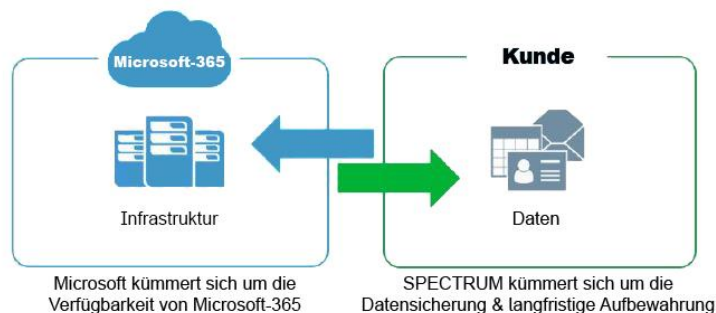
10 Jahres Managed-Backup (Datensicherung)

- tägliche Sicherung der kompletten Microsoft-365-Daten
- Automatische Überwachung der täglichen Datensicherung und zusätzliche Überprüfung durch die IT-Profis von SPECTRUM (Managed Service)
- die tägliche Datensicherung erfolgt nachts in einer Inkremental-Sicherung der veränderten Daten auf ein S3-Storage-System in einem Rechenzentrum in Deutschland
- die Daten werden mit einem nachlaufenden „Schweif“ von 10 Jahren gesichert
- die Backup-Datensicherung wird sicher und verschlüsselt auf dem S3-RZ-Storage-System gespeichert (S3 = sog. „Simple-Storage-Service“-Technik, dies ist ein Objekt-Speicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet).

Darüberhinaus können neben dieser Standard-„SPECTRUM-Backup-365“-Datensicherung auch andere Datensicherungsaufbewahrungszeiten vereinbart werden (diese müssen in Vertrags-Textform zwischen SPECTRUM und dem Auftraggeber spezifiziert werden).

Beschreibung der Datensicherung

Mit einer speziellen Datensicherungssoftware (Veeam) für die Microsoft-365-Umgebungen erfolgt jede Nacht die Datensicherung.



Die Daten werden mit einem sogenannten nachlaufenden "**Sicherungs-Schweif**" von **10 Jahren** gesichert. Während dieser Zeit können mit diesem Sicherungsverfahren Tag genau Daten aus MS-Outlook/Exchange-Online, MS-Teams, MS-OneNote, MS-OneDrive und MS-SharePoint-Online wiederhergestellt werden.

Für die Effizienz der Datenübertragung und Speicherung wird ein inkrementelles Backup-Verfahren verwendet. Nach dem initialen vollständigen Backup, bei dem eine Kopie aller ausgewählten Microsoft-365-Daten erstellt wird, wird bei den folgenden Backups nur noch ein inkrementelles Backup der Veränderungen/Differenzen durchgeführt. Das bedeutet, dass nur die Änderungen seit dem letzten Backup gespeichert werden. Dies reduziert sowohl die benötigte Bandbreite für die tägliche Datensicherung als auch den benötigten Speicherplatz.

Um die Sicherheit der Daten während der Übertragung und Speicherung zu gewährleisten, werden die Daten nach dem Advanced-Encryption-Standard-Verfahren (AES-256) verschlüsselt und komprimiert archiviert. Alle Daten werden während des gesamten Backup- und Wiederherstellungsprozesses sicher verschlüsselt abgelegt und übertragen. Ihre Backupdaten sind verschlüsselt in einem deutschen

Rechenzentrum abgelegt. Einzelne Datensätze (z.B. ein spezifisches Exchange-Postfach, eine E-Mail o.ä. können nicht aus der Gesamtdatensicherung eliminiert werden.

Hinweis: Mit „SPECTRUM-Backup für M365“ können natürlich nur die Daten gesichert bzw. rückgesichert werden, die Microsoft mit den verfügbaren M365-Lizenzen und die die Backup-Software Veeam zulässt. Die Spezifikation hierzu finden Sie unter:

www.spectrum-news.de unter „Kunden-Infos“ und „Leistungsbeschreibung“.

Sicherheit

Testweise führt SPECTRUM in Zeitabständen Rücksicherungen durch, um zu überprüfen, ob das Sicherungsverfahren auch einwandfrei für ggfs. benötigte Rücksicherungen funktioniert.

Die täglichen Datensicherungs-Läufe werden außerdem über automatisierte Managed-Service-Systeme und automatisierte Monitor-Verfahren laufend überprüft und die Datensicherungen werden täglich von den IT-Profis von SPECTRUM administriert und überwacht. Sollten Datensicherungen einmal nicht ordnungsgemäß durchgelaufen sein, werden diese umgehend händisch nachgeholt.

Alle Backup-S3-Storages befinden sich in einem deutschen Rechenzentrum und sind von den aktiven Arbeitssystemen der Auftraggeber grundsätzlich abgeschottet. Hierdurch wird verhindert, dass z.B. Verschlüsselungs- oder Backdoor-Erpressungs-Trojaner an diese Datensicherungen gelangen können.

Daten-Rücksicherungen

Datenrücksicherungen sind nicht Bestandteil der monatl. Sicherungspauschale. Sie werden nach tatsächlichem Zeitaufwand separat nach Aufwand zu den SPECTRUM-Stundensätzen den Kunden in Rechnung gestellt.

Hierbei ist zu erwähnen, dass z.B. die Rücksicherung einer Datei vom Vortag zumeist eine einfache Aktion von nur wenigen Minuten ist. Eine Rücksicherung eines Outlook-Postfaches aus dem Vormonat aber ggfs. schon einmal je nach Größe 1-3 Stunden dauern kann. Die tatsächlichen Aufwendungen werden zu den jeweils gültigen SPECTRUM-Stundensätzen laut Preisliste dem Auftraggeber in Rechnung gestellt.

Wartungsfenster „Typ Datensicherungszeit“

Die Sicherung der M365 Daten erfolgt in der Zeit von 21:00 bis 6:30 Uhr. Werden andere Datensicherungszeiten gewünscht, werden diese in Textform zwischen Auftragnehmer und dem Auftraggeber vereinbart.

Datensicherungs-Vertragsbeendigung

Kündigt der Auftraggeber den „SPECTRUM-Backup für Microsoft 365“-Datensicherungsvertrag löscht SPECTRUM bzw. eSPECTRUM unmittelbar nach Vertragsbeendigung die Backup-Daten.

Leistungsabrechnung / Vertragsabschluss

Das Produkt „SPECTRUM-Backup für Microsoft 365“ ist eine Entwicklung der SPECTRUM-Schwesterfirma **eSPECTRUM Internet-Solution GmbH**.

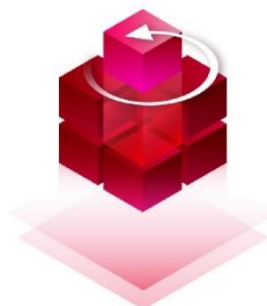
Backup-Verträge werden Daher mit der Firma eSPECTRUM und dem Auftraggeber abgeschlossen und monatl. von eSPECTRUM berechnet. Die Zahlungsweise erfolgt nach dem SEPA-Lastschriftverfahren. Die Abrechnung für die Datensicherung „SPECTRUM-Backup für M365“ erfolgt auf Basis der „SPECTRUM-Backup für M365“-Preisliste.

Die Haftung auf Schadensersatz, gleich aus welchem Rechtsgrund, ist ausgeschlossen; eine verschuldensunabhängige Haftung für anfängliche Mängel auf Schadensersatz besteht nicht. Dies gilt auch für die persönliche Haftung der gesetzlichen Vertreter, Mitarbeiter und Erfüllungsgehilfen von SPECTRUM bzw. eSPECTRUM. Ansonsten gelten die Allg. Geschäftsbedingungen AGB. SPECTRUM haftet nicht für Fehler seitens Veeam, Microsoft oder Wasabi.

Die Mindestvertragslaufzeit beträgt 12 Monate und ist danach zum Quartalsende (d.h. zum 31.3., 30.6., 30.9. oder 31.12. eines jeden Jahres) mit einer Kündigungszeit von 6 Wochen zum Quartalsende kündbar.



Schutz Ihrer Microsoft 365-Daten vor versehentlicher Löschung, Sicherheitsbedrohungen und Lücken in Aufbewahrungsrichtlinien



Schnelle Wiederherstellung einzelner Microsoft 365-Objekte und -Dateien mit branchenführenden, flexiblen Optionen



Einhaltung gesetzlicher Bestimmungen und Compliance-Vorgaben mit effizientem e-Discovery von Microsoft 365-Backup-Archiven

Warum ein SPECTRUM-Backup für Microsoft-365 ?

MS-Outlook/Exchange, MS-Teams, MS-OneNote, MS-OneDrive, MS-SharePoint-Online & Co. gehören u.a. zu den cloudbasierten Apps aus der Microsoft-365-Suite. Viele Unternehmen arbeiten heute schon mit diesen Apps aus Microsoft-365. Viele glauben aber, dass Microsoft auch die Daten in der Cloud mit absichert. Dies ist ein großer Irrtum – das stimmt leider nicht: Microsoft stellt nur die Infrastruktur zur Verfügung – für die Datensicherung in Microsoft-365 sind die Kunden selbst verantwortlich.

Sie benötigen ein Backup für Ihre Microsoft-365-Daten:

- Zur Datenverlust Prävention: Selbst in der Cloud sind Ihre Daten vor menschlichen Fehlern, Hackerangriffen oder technischen Fehlern nicht völlig sicher.
- Aus rechtlichen Compliance-Gründen: Viele Branchen erfordern regelkonforme Datensicherungen und Archivierungen, um gesetzlichen und regulatorischen Anforderungen zu genügen.
- Um die Geschäftskontinuität bei IT-Störungen zu gewährleisten: In kritischen Momenten ermöglicht ein Backup den schnellen Zugriff bzw. ein Restore auf wichtige Daten und sichert so den ununterbrochenen Geschäftsbetrieb.

Der Kunde hat beim Einsatz von Microsoft-365 selbst die Verantwortung für die Daten!