Whitepaper

Cloud-Backup für Microsoft 365

Erfolgreich arbeiten – dank geschützter Daten

Cloud Backup: Zuverlässige Absicherung gegen Datenverluste

vodafone business

Together we can

Datenverluste können hohe Kosten und Betriebsstillstände verursachen

246 Mio.

Versuche von Informationsdiebstahl beobachtet Cisco an jedem Tag.
(Seite 5)

4,6 Mio. US-$

durchschnittliche Kosten entstehen laut IBM und Ponenom Institut bereits bei einem Datenverlust, der nur eine geringe Geschäfts-unterbrechung zur Folge hat.
(Seite 6)

bis zu 600.000 €

waren laut Semperis die Lösegeldsumme, die 89% der befragten Unternehmen nach einem erfolgreichen Ransomware-Angriff bezahlt haben.
(Seite 6)

206 Tage

sind laut IBM der durchschnittliche Zeitraum zwischen der Kompromittierung von Daten und deren Entdeckung.
(Seite 9)

65%

der befragten weltweiten Großunternehmen haben wenig Vertrauen, dass ihr Unternehmen im Falle eines Datenverlusts die Systeme/Daten auf allen genutzten Plattformen vollständig wiederherstellen kann.
(Seite 4)

Vorwort

Unternehmen müssen sich aus ihrem ureigensten Interesse gegen Datenverluste wappnen. Dabei sollten sie auch Microsoft 365 im Blick behalten.

In vielen deutschen Unternehmen sind die Kommunikations-, Bürosoftware- und Zusammenarbeits-Lösungen von Microsoft die Basis der täglichen Geschäftsprozesse. Allerdings unterschätzen viele geschäftliche Anwendende, dass die Bordmittel dieser Lösungen zur Datensicherung für eine Vielzahl von Bedrohungen und Szenarien gar nicht ausgelegt sind.

Demgegenüber stehen wachsende Risiken für Datenverluste. Sie reichen von versehentlicher oder böswilliger Löschung durch Mitarbeitende – sei es als Konsequenz von Stress und Überforderung oder als Vergeltungsmaßnahme beispielsweise nach einer Kündigung – bis zu den vielfältigen Bedrohungen durch Cyberangriffe.

Der Verlust von Projektdaten, Kontakten, Terminen oder anderen Dateien bedroht die Arbeitsfähigkeit des gesamten Unternehmens. Hinzu kommen gesetzliche Anforderungen an die Datensicherheit und -Verfügbarkeit sowie externe und interne Compliance-Vorgaben. Microsoft selbst weist darauf hin, dass Unternehmen selbst für eine regelmäßige Datensicherung sorgen müssen.

Wie geeignete Backup-Strategien für die genannten Daten aussehen und was geschäftliche Nutzer:innen in diesem Zusammenhang wissen sollten, haben wir im vorliegenden Whitepaper für Sie zusammengestellt.

Inhaltsverzeichnis

1 Digitales Arbeiten erfordert gezielten Schutz der Daten in der Cloud

Längst gehört es zum Unternehmensalltag, dass die Mitglieder eines Teams gemeinsam Dokumente bearbeiten – oder auch zusammen mit ihren Kund:innen. Dabei können sich alle Teilnehmer :innen an beliebigen Orten befinden – etwa **unterwegs oder im Homeoffice**.

Möglich wird das durch eine **zentrale Datenspeicherung in der Cloud.** Die Bürosoftware **Microsoft 365**, die weltweit rund 100 Millionen Nutzer:innen in Unternehmen aller Größenordnungen hat, unterstützt dies. Zum Beispiel mit ihren Funktionen zur Zusammenarbeit wie die Cloud-Dateiablage OneDrive oder die Kollaborations-Umgebung SharePoint. Dabei ist es **von zentraler Bedeutung, dass die Datenbestände sicher verwaltet werden.** Denn es handelt sich häufig um sensible Inhalte, Unternehmens-Know-how und personenbezogene Informationen.

Stünden die in der Cloud gespeicherten Dokumente, E-Mails, Projektdaten, Termine, Aufgaben und Diskussionen nicht mehr zur Verfügung, könnte dies **hohe Verluste** verursachen – und im schlimmsten Fall **die Existenz des Unternehmens bedrohen.**

Unternehmen sehen sich nicht gut gegen Datenverluste gewappnet

Der Anbieter Dell berichtet in seiner Studie „Global Data Protection Index 2024“ [1]: **60% der befragten weltweiten Großunternehmen haben kein großes Vertrauen in die Backup- und Recovery-Lösung in ihrem Haus.** Sollte es zu einem Datenverlust kommen, sind 65% skeptisch, dass sich alle Daten auf allen Plattformen wiederherstellen lassen. Das ist besonders kritisch, da 75% besorgt sind, ob ihre Organisation ausreichend gegen Malware- oder Ransomware-Bedrohungen gewappnet ist.

60%

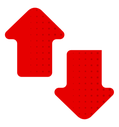
haben **kein großes Vertrauen**, dass ihre Organisation ihre **eigenen Service-Level-Vorgaben** (Service Level Objectives – SLOs) **für Backup und Wiederherstellung erfüllt.**

79%

befürchten, dass ihr Unternehmen **in den nächsten 12 Monaten von einem disruptiven Ereignis** (wie Cyberangriffen oder größeren Datenverlusten) **betroffen** sein wird.

75%

befürchten, dass die **bestehenden Datenschutzmaßnahmen** ihres Unternehmens nicht ausreichen, **um Bedrohungen durch Malware und Ransomware zu begegnen**.



65%

haben **kein großes Vertrauen**, dass ihr Unternehmen **im Falle eines Datenverlusts** die **Systeme/Daten auf allen genutzten Plattformen vollständig wiederherstellen** kann.

[1] Quelle: https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf

2 Ursachen und Risiken von Datenverlusten

Die Ursachen für Datenverluste sind vielfältig und reichen von versehentlichem Löschen über absichtliche Sabotage bis hin zu Hackerangriffen. Für die Folgen spielt es aber nur eine untergeordnete Rolle, ob der Verlust wichtiger Daten auf einen Cyberangriff oder versehentliche bzw. absichtliche Aktionen eigener Mitarbeitender zurückgeht.

Datenverluste durch Cyberangriffe

Den Wert von Unternehmensdaten haben auch Cyberkriminelle immer stärker im Visier, um sich beispielsweise durch digitale Lösegelderpressung zu bereichern. Gemäß dem „Cyber Threat Trends Report“ [1] von Cisco belegen **Informationsdiebstahl, Trojaner und Ransomware die Top 3 unter den Cyber-Bedohungen**. Definitionen der verschiedenen Malware-Kategorien finden Sie im Glossar auf Seite 16.
Dabei dürfen sich kleine und mittlere Unternehmen nicht in falscher Sicherheit wiegen und denken, dass sie für Sabotage oder Hackerangriffe uninteressant seien. Laut der HDI Cyberstudie 2024 [2] **konzentrieren sich Cyberangriffe zunehmend auf den Mittelstand**, also Firmen mit 50 bis 250 Mitarbeitenden, **sowie auch Kleinunternehmen**. Dabei profitieren die Angreifer davon, dass Unternehmen dieser Größenordnungen in der Regel weniger leistungsfähige Abwehrlösungen einsetzen.

Datenlöschung durch Mitarbeitende

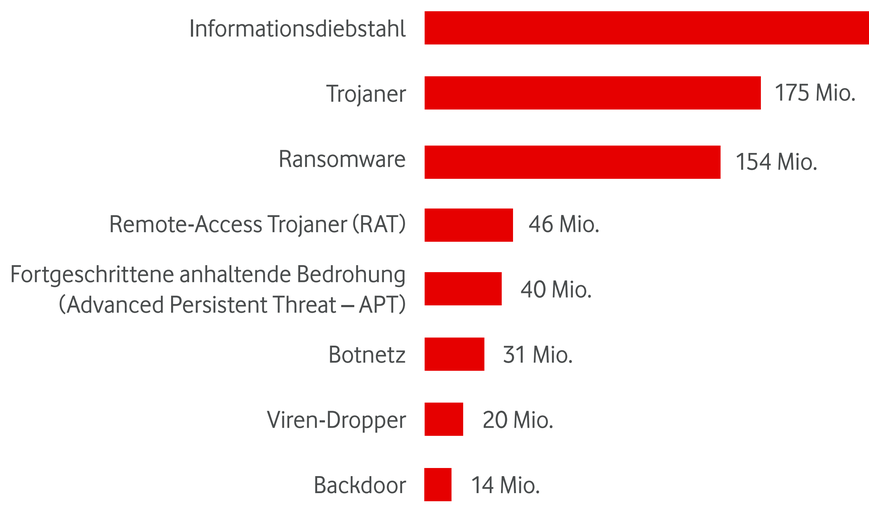
Cyberangriffe sind somit eine reale, aber keineswegs die einzige Ursache für Datenverluste. Schnell kann ein Mitarbeitender **ungewollt und versehentlich eine Datei, E-Mail oder ganze Verzeichnisse löschen.** In einer immer komplexeren Arbeitswelt sind **Stress und Überlastung** einer der **Hauptgründe für Datenverlust**.[3] Hinzu kommen **Risiken, die von unzufriedenen Mitarbeitenden** ausgehen. Hierbei ist besonders kritisch, dass Löschungen im Rahmen normaler Benutzeroperationen oft gar nicht als Bedrohung erkannt werden.

Datenverlust durch Fehlfunktionen

Außerdem können auch **Software- oder Hardwareprobleme** oder irrtümliche/fehlerhafte **Änderungen an Konfigurationen** zu Datenverlusten führen. Dazu zählen etwa das Überschreiben von Dokumenten oder der unwiderrufliche Verlust des Zugriffs auf Daten.

Die Top 3 der Bedrohungen: Informationsdiebstahl, Trojaner und Ransomware

Durch Analyse von über 700 Milliarden DNS*-Anfragen pro Tag bestimmt Cisco in seinem „Cyber Threat Trends Report“ die im IT-Alltag am häufigsten auftretenden Bedrohungskategorien. Hier die Auswertung für 2024:



* DNS = Domain Name System – DNS-Server übersetzen Webadressen in IP-Adressen und sind daher ein idealer Ausgangspunkt für Analysen des weltweiten Internet-Verkehrs

[1] Quelle: https://umbrella.cisco.com/info/cyber-threat-trends-report

[2] Quelle: https://www.hdi-brandportal.com/share/XMPYmLs9nXGviujFAWdb/assets/49122

[3] Quelle: https://www.mimecast.com/de/resources/ebooks/state-of-human-risk-2025

3 Weitreichende Konsequenzen von Datenverlusten

Interne Konzepte, Strategien, Kund:innen- und Finanzdaten – im Arbeitsalltag haben Daten einen enormen Wert für Unternehmen. Unabhängig von den Ursachen hat ein Verlust solcher Daten gravierende Folgen.

Hohe Kosten durch Datenverluste

In ihrem „Cost of a Data Breach Report“ [1] belegt IBM, dass die **Kosten eines Datenverlusts** je nach Grad der Geschäftsunterbrechung im Durchschnitt der befragten Unternehmen **zwischen 4,6 und 5 Millionen US-Dollar** betragen. In **Deutschland** betrug der **Gesamtschaden** laut dem Branchenverband Bitkom [2] im Jahr 2024 **267 Milliarden Euro** – davon 179 Milliarden Euro durch Cyberattacken.

Weitere Folgeschäden und -kosten

Hinzu kommt, dass die beschriebenen Vorfälle auch in erheblichem Maße zu Geschäftsunterbrechungen führen. In der oben genannten IBM-Studie geben **52 Prozent** der Befragten an, dass der Datenverlust zu einer **wesentlichen Unterbrechung der Geschäftstätigkeit** geführt hat. **18 Prozent** wählten sogar die Antwort „**sehr wesentlich**“.

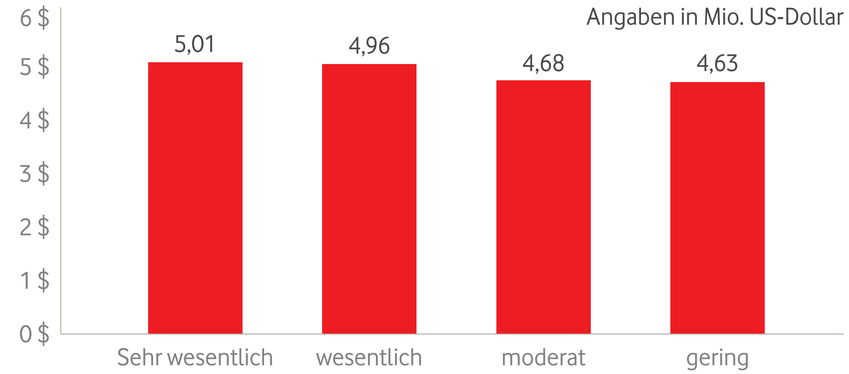
Daraus folgen neben Einnahmeausfällen auch Einschnitte beim Vertrauen der Kund:innen, Terminverschiebungen, Ausfälle bei der Nutzung von Geschäftschancen, der Verlust von Kund:innen oder Anschlussgeschäften und gegebenenfalls auch noch Strafzahlungen.

Kosten durch Cyberangriffe

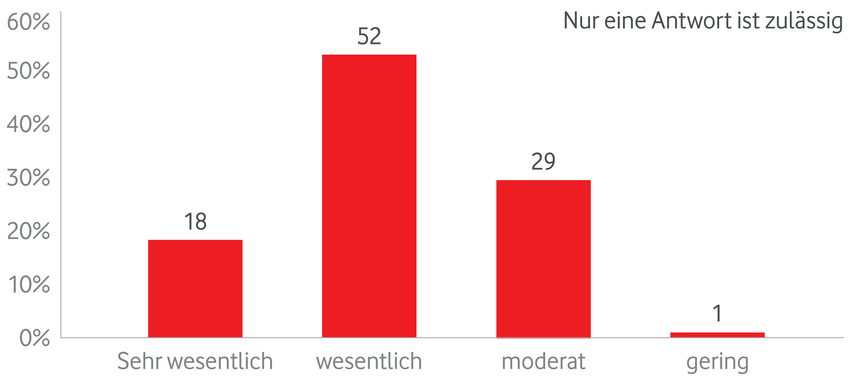
Auch wenn Sicherheitsexpert:innen bei Ransomware-Angriffen von der Zahlung von Lösegeldern abraten, könnten drohende hohe Kosten manche Unternehmen doch dazu bewegen, eine Zahlung zu leisten. Laut dem „Ransomware Report“ [3] des Sicherheitsunternehmens Semperis haben **78 Prozent der** von einem solchen Angriff **betroffenen Unternehmen Lösegeld gezahlt**. **35 Prozent** der Zahlenden **erhielten dennoch keinen Zugriff auf ihre verschlüsselten Daten**. Befragt wurden insgesamt 900 IT- und Sicherheitsexpert:innen verschiedener Branchen aus den USA, Großbritannien, Frankreich und Deutschland. In Deutschland zahlten 89 Prozent der betroffenen Unternehmen **insgesamt bis zu 600.000 Euro an Lösegeld**, bei den übrigen 11 Prozent wurde diese Grenze sogar überschritten.

Kosten eines Datenverlusts basierend auf dem Grad der Geschäftsunterbrechung

IBM und das Ponemon Institut haben Cybersicherheits- und IT-Verantwortliche in 604 Organisationen befragt, die 2023 von einem Datenverlust betroffen waren.



In welchem Umfang hat der Datenverlust zu Geschäftsunterbrechungen geführt?



[1] Quelle: https://www.ibm.com/reports/data-breach
[2] Quelle: https://www.bitkom.org/Presse/Presseinformation/10-Milliarden-Euro-Deutschlands-Cybersicherheit
[3] Quelle: https://www.semperis.com/de/ransomware-risk-report

4 Compliance-Anforderungen und Haftungsrisiken

Zu den Gefahren für den laufenden Geschäftsbetrieb und für die Handlungsfähigkeit des Unternehmens kommen erhebliche Haftungsrisiken.
Relevant sind in diesem Zusammenhang etwa die europäische **Datenschutzgrundverordnung (DSGVO)**, aber auch nationale Gesetze wie das sogenannte **BSI-Gesetz (BSIG,** BSI = Bundesamt für Sicherheit in der Informationstechnik) – siehe rechte Spalte. Unter anderem fordert die DSGVO, dass **personenbezogene Daten bei einem Zwischenfall unverzüglich wiederherzustellen sind** (Art. 32 DSGVO).

EU-weite Richtlinie NIS2

Die EU-Richtlinie 2022/2555 (NIS2), auf deren Basis alle EU-Mitgliedstaaten eine entsprechende nationale Gesetzgebung erlassen müssen, fordert **weitreichende technische, organisatorische und operative Risikomanagement-Maßnahmen**. Die wesentliche Frage für Unternehmen lautet, ob sie **von NIS2 betroffen sind oder nicht**. Dafür gibt es **zwei Kriterien**:

- In welchem **Wirtschaftssektor** ist das Unternehmen tätig? NIS2 benennt Sektoren wie etwa Energie, Verkehr und Transport, Bank- und Finanzwesen.
- Die **Unternehmensgröße**. Dabei wird zwischen „**besonders wichtigen Einrichtungen**" und „**wichtigen Einrichtungen**" unterschieden – für Letztere sind geringere Geldstrafen vorgesehen und die Behörden haben etwas weniger Durchgriffsmöglichkeiten.

Neben möglichen **hohen Bußgeldern ist** eine **explizite Haftung der Geschäftsführung** vorgesehen. In gravierenden Fällen ist sogar ein **temporäres Absetzen der Geschäftsleitung** möglich.

Branchenspezifische Anforderungen

In verschiedenen Branchen gelten darüber hinaus spezifische Anforderungen, z.B. die **HIPAA**-Regelungen (Health Insurance Portability and Accountability Act) **in der Gesundheitsbranche** oder **SOC2** (Service Organization Control 2) **in der Finanzbranche**.
Zudem gilt **branchenübergreifend die Norm ISO/IEC 27001** für Informationssicherheits-Managementsysteme.
Die jeweiligen Regelungen haben unterschiedliche Schwerpunkte. Gemeinsam fordern sie jedoch die **Einhaltung von Vertraulichkeit und Privatsphäre bei gleichzeitiger Sicherstellung der Verfügbarkeit und Integrität der Daten**.

§ Geforderte Cybersicherheits-Maßnahmen (§30 BSIG)

- Risikoanalyse und -management
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Business Continuity (u. a. Backup Management, Wiederherstellung) und Krisenmanagement
- Sicherheit in der Lieferkette
- Sichere Entwicklung, Beschaffung und Wartung von IT
- Wirksamkeitsprüfungen der Risiko- und IT-Sicherheitsmaßnahmen
- Cyber-Hygiene und Schulungen
- Kryptographie und Verschlüsselung
- Sicherheit des Personals und Zugriffskontrolle
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung sowie gesicherte Kommunikationskanäle

5 Umfang und Grenzen der in Microsoft 365 enthaltenen Datensicherung

Als am weitesten verbreitete Bürosoftware und Plattform für die Zusammenarbeit von Teams, ist auch Microsoft 365 von der Problematik der Datensicherung betroffen. Aufgrund seiner hohen Marktbedeutung konzentriert sich die nachfolgende Betrachtung gezielt auf dieses Software- und Cloud-Paket.

In seiner **Standardausstattung bietet Microsoft 365 Funktionen zur Sicherung und Wiederherstellung** von Daten. Allerdings bedeuten diese Funktionen **keinen umfassenden Schutz gegen alle zuvor beschriebenen Bedrohungen.**

Microsoft weist deshalb in seinem Servicevertrag selbst **darauf hin**, dass es in der Verantwortung der Nutzer:in bzw. Unternehmens liegt, **regelmäßig Sicherungskopien aller relevanten Daten zu erstellen**.

Spiegelung versus Kopie

Wie andere Cloud-Dienste bietet Microsoft 365 **Geo-Redundanz.** Die Daten werden in verschiedenen Rechenzentren gespiegelt, sodass sie gleichzeitig an mehreren Speicherorten vorliegen. Dies **schützt vor dem Ausfall eines dieser Zentren, aber nicht vor Datenverlusten durch andere Ursachen.** Denn der Zustand der Daten vor einer Veränderung wird dadurch nicht gesichert. Und wenn Mitarbeitende zum Beispiel Daten löschen, versehentlich verschieben oder beschädigen, wird diese Aktion in Echtzeit an allen Standorten synchronisiert.

Auf der nächsten Seite beleuchten wir, welche Funktionen in Microsoft 365 enthalten sind und wo deren Grenzen liegen.

Eingeschränkter Schutz durch die Bordmittel von Microsoft 365

Abgesichert

- Verfügbarkeit der Daten durch Geo-Redundanz
- Papierkorb-Funktion zum Rückgängigmachen versehentlicher Löschungen

Nicht abgesichert

- Zustand der Daten vor Datenverlust
- Absichtliche Löschung durch Benutzer:in bzw. Administrator:in

„Wir empfehlen Ihnen dringend, regelmäßig Sicherungskopien Ihrer Inhalte zu erstellen."

Auszug aus dem Microsoft-Servicevertrag (https://www.microsoft.com/de-de/servicesagreement)

5 Umfang und Grenzen der in Microsoft 365 enthaltenen Datensicherung

Doch wo genau liegen die Probleme der Einschränkungen, die auf Seite 8 beschrieben wurden?

Begrenzte Möglichkeiten zur Wiederherstellung

Daten, die in Microsoft 365 gelöscht wurden, werden je nach Anwendung, Lizenz und Konfiguration **für einen begrenzten Zeitraum in den Papierkörben** etwa von SharePoint und Exchange gespeichert. Dabei gelten relativ kurze Aufbewahrungszeiten (siehe rechte Spalte).

Dies kann sich nicht zuletzt bei Cyberangriffen oder anderen Datenverlusten als problematisch erweisen, wenn diese ggf. erst später erkannt werden. Hinzu kommt: Wird ein Papierkorb endgültig gelöscht, verliert er seine Wiederherstellungsfunktion. Eine **versehentliche oder absichtliche dauerhafte Löschung** von Daten aus einem „OneDrive for Business"-Account durch Endnutzer – oder etwa auch von SharePoint-Website-Daten durch eine SharePoint-Administrator:in **lässt sich nicht rückgängig machen.**

Auch eine Versionierung der Dokumente bietet allein keinen zuverlässigen Schutz, denn mit dem endgültigen Löschen einer Datei werden auch deren frühere Versionen gelöscht.

Ist eine Wiederherstellung über die Bordmittel von Microsoft 365 nicht mehr möglich, bleiben als letzter Ausweg **historische Sicherungskopien** im Rechenzentrum. Aus ihnen lassen sich die Inhalte aus einer letzten als fehlerfrei bekannten Version wiederherstellen. Doch eine **Wiederherstellung auf diesem Weg ist zeitintensiv** – sie kann **mehrere Tage** in Anspruch nehmen. Zudem **setzen Funktionen wie eine rechtssichere Archivierung teurere Office-365-Lizenzen voraus.**

Zeitliche Limitierung problematisch

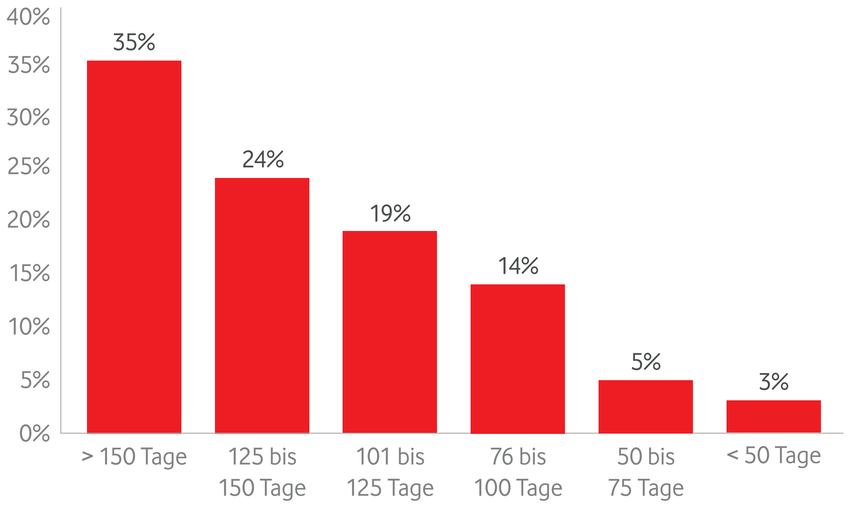
Gerade die zeitlichen Limitierungen stellen ein erhebliches Risiko dar. Denn laut einer Studie von IBM beträgt der **durchschnittliche Zeitraum zwischen der Kompromittierung von Daten und deren Entdeckung 206 Tage**. Dies spiegelt sich auch in dem ebenfalls von IBM veröffentlichten „Cost of a Data Breach Report" [1], wonach die durchschnittliche Zeit bis zur Wiederherstellung nach einem Datenverlust in 35% der Fälle mehr als 150 Tage dauert.

Aufbewahrungszeiten der Papierkorb-Funktion von Microsoft 365

Microsoft Exchange: **max. 30 Tage**

Groups, Microsoft Teams,
SharePoint & OneDrive for Business: **93 Tage**

Durchschnittliche Zeit bis zur Wiederherstellung nach einem Datenverlust

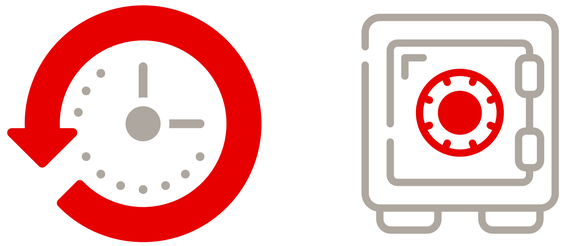


[1] Quelle: https://www.ibm.com/downloads/cas/OJDVQGRY
[2] Quelle: https://www.ibm.com/reports/data-breach

6 Backup vs. Archivierung

Unternehmen unterliegen in der Regel **gesetzlichen Aufbewahrungsfristen** – etwa für steuerlich relevante Buchhaltungsdaten oder bestimmte digitale Aufzeichnungen über Geschäftsvorgänge. Diese rechtlichen Verpflichtungen werden durch **Archivierungslösungen** erfüllt. Sie legen ausschließlich die hierfür relevanten Daten in bestimmten Intervallen auf dauerhaften Speicherlösungen ab, die für lange Aufbewahrungszeiträume geeignet sind – in der Regel zehn Jahre. Je nach Anforderungen setzen Unternehmen daher gegebenenfalls neben Backup-Lösungen auch eine Archivierungsfunktion ein. Da beide Lösungen unterschiedliche Zielsetzungen verfolgen, liegen bei Backups üblicherweise kürzere Intervalle zwischen den Sicherungen als bei Archivierungslösungen.

Werden Daten zur langfristigen Aufbewahrung archiviert, beinhaltet dieser Prozess häufig, dass sie anschließend von den im Produktionsbetrieb genutzten Speichersystemen gelöscht werden. Dies kann bedingen, dass **Archive die jüngsten Daten laufender Projekte und Geschäftsvorfälle noch gar nicht beinhalten.**



Verschiedene Zielsetzungen: Backups „drehen die Zeit zurück", bei einer Archivierung kommen die Daten zur dauerhaften Aufbewahrung „in den Safe".

Unterschiedliche Konzepte: Backup und Archivierung

Lösung	Umfang der Datensicherung	Anwendungsszenario	Kosten	Komplexität
Backup	Kurz- und mittelfristig. Mehrere automatische Datensicherungen täglich	Schutz von Daten und Produktivität durch schnelle Wiederherstellung verlorener Daten	gering	gering bis mittel
Archivierung	Langfristig. Separate Sicherung und dauerhafte, revisionssichere (vor Veränderungen geschützte) Aufbewahrung	Gegebenenfalls zur Erfüllung gesetzlicher Vorschriften erforderlich	mittel bis hoch	mittel bis hoch

7 Auswahlkriterien für Microsoft-365-Sicherungslösungen

Um Datenverluste innerhalb der Daten- und Verwaltungsstruktur von Microsoft 365 optimal zu sichern, ist eine dafür gezielt ausgelegte Backup-Lösung empfehlenswert. Welche Kriterien bei der Auswahl einer solchen Lösung relevant sind, wird im Folgenden näher beleuchtet.

Sicherung aller Daten von Microsoft 365

Eine wichtige Anforderung an Datensicherungslösungen ist, dass diese **permanent und ohne Benutzerinteraktion im Hintergrund** ablaufen. Zudem müssen **alle relevanten Daten davon abgedeckt** sein. In der Regel sollten daher alle Komponenten von Microsoft 365 einbezogen werden – insbesondere auch die Szenarien für Zusammenarbeit wie Microsoft Teams. Abhängig vom Umfang bereits bestehender Sicherungslösungen kann es aber auch eine sinnvolle Strategie sein, ergänzend gezielte Einzelelemente wie zum Beispiel E-Mails oder Dateiablagen zu sichern.

Verschlüsselung der Backup-Daten

Um den Anforderungen der DSGVO und anderen gesetzlichen Vorschriften gerecht zu werden, müssen **personenbezogene Daten verschlüsselt gespeichert** werden. Ratsam ist daher, die kompletten **Backup-Daten mit starker Verschlüsselung** abzulegen. Auch während der **Übertragung auf Cloud-Server** sollte bereits eine **Ende-zu-Ende-Verschlüsselung** stattfinden.

Frequenz der täglichen Backups

Steigt die **Anzahl der automatischen Backups pro Tag,** wird dadurch der Zeitraum zwischen dem letzten Backup und dem Datenverlust reduziert. Eine **hohe Frequenz stellt sicher**, dass die benötigte Information in einer Fassung wiederhergestellt werden kann, die **Weiterarbeiten ohne Produktivitätsverlust schnell ermöglicht.**

Schnelligkeit der Wiederherstellung

Je **schneller die Suche nach Daten** und die zugehörige Wiederherstellung erfolgt, **umso kürzer bleiben die Auswirkungen auf die Produktivität.**

Deshalb sollte die eingesetzte Lösung flexibel auf unterschiedliche Szenarien reagieren können – dies beleuchten wir auf der folgenden Seite.

Überlegungen zur Datensicherung

- Welche Daten sollen gesichert werden?
- Welche Anforderungen hat das Unternehmen in Bezug auf Gesetze und Vorschriften?
- Welche Anforderungen müssen im Hinblick auf Datenverschlüsselung erfüllt werden?
- Werden Teile der benötigten Daten durch eine vorhandene Datensicherungslösung bereits abgedeckt?

Überlegungen zur Geschwindigkeit und Aktualität der Datenwiederherstellung

- Wie viele Stunden, in denen auf verlorene Daten nicht zugegriffen werden kann, kann sich das Unternehmen leisten?
- Wie schnell müssen die Daten nach Entdecken eines Verlusts wieder bereitgestellt werden?
- Welche Instanz im Unternehmen ist für die Wiederherstellung zuständig?
- Wie soll der Ablauf nach Entdecken eines Datenverlusts aussehen (zum Beispiel Ticket beim IT-Support)?

7 Auswahlkriterien für Microsoft-365-Sicherungslösungen

Wie auf der vorherigen Seite beschrieben, sollte die Backup-Lösung die benötigten Daten flexibel wiederherstellen können.

Grundsätzlich gilt: **Daten müssen an ihrem ursprünglichen Ort wieder bereitgestellt werden können – und zwar exakt ab dem benötigten Zeitpunkt.** Dazu sollte die gewählte Backup-Lösung die rechts aufgeführten **Wiederherstellungsoptionen** anbieten.

Wichtig ist außerdem ein **Cross-User Restore.** Er stellt alle Daten eines Users einem anderen User gebündelt zur Verfügung.

Gesamt- oder Einzelwiederherstellung: Es müssen genau die benötigten Daten wiederhergestellt werden – von einzelnen Dokumenten bis hin zu ganzen Ordnern, Listen oder kompletten Gruppen oder Sammlungen am Standort der Daten.

Übergreifende Wiederherstellung eines Postfachs: Daten müssen sich aus einem Postfach wiederherstellen lassen und sollten dabei in ein anderes verschoben werden können, wenn dies erforderlich ist (zum Beispiel nach Weggang eines Mitarbeitenden).

Point-in-Time-Wiederherstellung: Daten sollten sich bis zu einem bestimmten Zeitpunkt wiederherstellen lassen. Dies ist insbesondere bei Ransomware-Angriffen entscheidend.

Diese Elemente müssen gesichert werden und sich vollständig wiederherstellen lassen

	Exchange Online	SharePoint Online	OneDrive for Business	MS Teams & Groups	Planner
Backup	• E-Mail, Kalender, Kontakte • Aufgaben, Notizen, Journal • Öffentlicher Ordner und Shared Mailboxes	• Klassische Team-Seiten • Unterseiten • Listen • Dateien und Dateiversionen	• Ganzer Account • Ordner • Dateien und Dateiversionen	• Kanäle: private & öffentliche • Teams Chat • Planner • Dateien und Dateiversionen	• Alle Pläne, Aufgaben, Buckets
Restore	• Einzeldatei oder Bulk • Vollständiges Postfach • Postfachübergreifend • Point-in-Time auch von Ordner und Dateien • Cross-Mailbox Restore	• Einzeldatei oder Bulk • Alle Seiten und Unterseiten • Point-in-Time auch von Ordnern und Dateien • Cross-Sharepoint Restore	• Einzeldatei oder Bulk • Vollständiger Account • Point-in-Time auch von Ordnern und Diensten • Cross-OneDrive Restore	• Einzeldatei oder Bulk • Ganze Teams und Kanäle • Posts und Chats • Cross-Teams Restore	• Einzeldatei oder Bulk • Gesamter Planner

8 Überlegungen zu Betriebskosten

Gesamtbetriebskosten

Die Auswahl einer Datensicherungslösung für Microsoft 365 muss **alle entstehenden Kosten berücksichtigen** – auch zunächst „unsichtbare“ wie Implementierung, Verwaltung und Speicherung.

Lösungen, bei denen **eine Abrechnung nach genutztem Speicherplatz erfolgt, machen die Kosten unkontrollierbar** – denn sie können im Laufe der Zeit enorm zunehmen.

Um die tatsächlichen Gesamtbetriebskosten einer Lösung zu ermitteln, sind alle Aufwände von der Installation bis zur laufenden Betreuung und Nutzung zu beachten:

Installation: Sind noch weitere Installationen in der IT-Umgebung des Unternehmens erforderlich?

Konfiguration: Wie einfach sind das Setup und die Anpassung von Einstellungen auf die eigenen Anforderungen des Unternehmens?

Dauer der Wiederherstellung: Wie lange dauert es nach der Entdeckung eines Datenverlusts, die Daten wiederherzustellen – und somit wieder Produktivität herzustellen?

Betrieb: Wie groß ist der Aufwand, die Lösung zu betreiben und dauerhaft an den Bedarf des Unternehmens und seiner Mitarbeitenden anzupassen?

Wachsende Speicherkapazität führt zu steigenden Kosten

Viele Backup-Lösungen für Microsoft 365 **rechnen nach dem verwendeten Speicherplatz ab**. Angesichts meist exponentiell wachsender Datenvolumen stellen solche Abrechnungsgrundlagen ein **hohes Kostenrisiko** dar. So berechnet das Beratungsunternehmen IDC [1] das weltweite Datenvolumen im Jahr 2025 mit 150 Zetabytes (Billionen Gigabytes bzw. Tausende Milliarden GB). Für das Jahr 2025 erwartet die Studie bereits 394 Zetabytes – und somit ein Anwachsen auf das Zweieinhalbfache.

IT-Administrator:innen sollten über das genutzte Datenvolumen informiert sein. Lösungen, die unbegrenzte Backups ohne Speicherbegrenzung erlauben, sind jedoch eine wichtige Versicherung gegen überraschende Kostenexplosionen.

[1] Quelle: https://my.idc.com/getdoc.jsp?containerId=US52076424

9 Maßgeschneiderte Lösung: Vodafone Cloud-Backup für Microsoft 365

Als zuverlässiger Partner für alle Aspekte der Digitalisierung bietet Vodafone seinen Geschäftskunden eine maßgeschneiderte Lösung für die Sicherung der in Microsoft 365 genutzten Datenbestände an: **Cloud-Backup für Microsoft 365.**

Diese Lösung erfüllt alle **Anforderungen an die Sicherung der Datenbestände von Microsoft 365** und **ergänzt damit die bordeigenen Sicherungsfunktionen des Microsoft-Pakets.** Sie bietet **unbegrenzten Speicherplatz** ohne zeitliche Beschränkung und ohne Abrechnung nach Datenvolumen.

Suche und Wiederherstellung verlorener Daten erfolgen **per Mausklick** ohne Installationsaufwand. **Gesamt- oder Einzelwiederherstellung**, **Übergreifende Wiederherstellung von Postfächern** und **Point-in-Time-Wiederherstellung** werden unterstützt.

Dabei werden die Daten **compliance-konform und sicher in deutschen Rechenzentren** gespeichert, was Unternehmen bei der Einhaltung der **DSGVO** unterstützt. **Alle diese Leistungen und Funktionen sind im Preis von Cloud-Backup für Microsoft 365 inkludiert.**

Wiederherstellung in wenigen Minuten nach versehentlicher Löschung

Dabei hat sich **Cloud-Backup für Microsoft 365 im praktischen Einsatz schon vielfach bewährt.** Dies zeigen auch die Erfahrungen mehrerer Unternehmen. Da es sich um geschäftskritische Datensicherheits-Vorfälle handelt, möchten die betroffenen Firmen jedoch nicht genannt werden.

So **löschte** ein **Mitarbeitender eines KMU versehentlich eine umfangreiche SharePoint-Bibliothek mit über 50.000 Dateien.** Die Wiederherstellung über die Papierkorb-Funktion hätte mehrere Tage gedauert, **Mit Cloud-Backup für Microsoft 365 ließ sich die gesamte Bibliothek binnen weniger Minuten wiederherstellen.**

Eine **Anwaltskanzlei** wurde nach dem unvorsichtigen Anklicken einer E-Mail durch einen ihrer Angestellten **Opfer einer Ransomware-Attacke.** Von der Verschlüsselung durch die Schadsoftware waren **über 44.000 Dateien auf SharePoint** betroffen. Dank Cloud-Backup für Microsoft 365 ließ sich der **komplette Datenbestand in wenigen Stunden wiederherstellen**.

Cyber-Bedrohungen? Cloud-Backup für Microsoft 365 schützt vor den Folgen von Ransomware-Angriffen

Ransomware: Schutzschild vor den Folgen
Cloud-Backup für Microsoft 365 archiviert die Daten zeitlich unlimitiert, 6 Backups täglich

Ihr Schutz in 4 Schritten im Falle einer Erpressung

1. (Auto-) Synchronisierung (Exchange & OneDrive) pausieren

2. Malware entfernen

3. Wiederherstellung der Daten mit Stand vor dem Ransomware-Angriff

4. Synchronisierung (wieder) starten

9 Maßgeschneiderte Lösung: Vodafone Cloud-Backup für Microsoft 365

Zudem gewährleistet Vodafone eine DSGVO-konforme, verschlüsselte Speicherung auf deutschen bzw. europäischen Servern:

- Sichere **Speicherung in Deutschland** oder Europa.
- Einhaltung der **gesetzlichen Bestimmungen (z.B. DSGVO)**.
- Zuverlässiges **Cloud-Backup mit 2048-Bit-Verschlüsselung** (256 Bit bei Ende-zu-Ende-Übertragungen)
- Moderne **App-Authentifikation**: Sicherer Zugriff unter Nutzung der neuesten Microsoft-APIs.

Auch Datenschutz für Microsoft 365 Copilot

Darüber hinaus werden auch die Daten gesichert, die Grundlage für den Einsatz von **Künstlicher Intelligenz wie Microsoft 365 Copilot** sind. Denn **bei Verlust dieser Daten** wäre der unternehmensspezifische **Einsatz von Copilot nicht mehr möglich**.

Cloud-Backup für Microsoft 365 im Überblick

	Vodafone Cloud-Backup für Microsoft 365	▶ Warum ist das relevant?
Produktabdeckung Microsoft 365	Komplettes Microsoft 365 + Planner	... umfassender Schutz aller relevanten Tools von Microsoft 365.
Storage: Wo und welche Bedingungen	Azure – in Deutschland. Unbegrenzter Speicher, unbegrenzte Aufbewahrung.	... 100% DSGVO und NIS2-konform. Zudem ISO 27001/27701, DataPro+ sowie CAS StarLevel 1&2. Daten werden – ohne Kundenwunsch – vom Anbieter niemals gelöscht. Viele Wettbewerber haben hier intransparente Bedingungen.
User Interface	Einfach	... reduziert Supportaufwand und ermöglicht Kund:innen, das Backup zu nutzen. Keine komplexen Schulungen nötig – für Lean IT.
Einfaches Setup	Ja – Customer Self Service	... Kund:in kann Backup binnen 10 Minuten aufsetzen und konfigurieren – auch hier: Lean IT.
Umfang des Datenschutzes	Alle 4h (6x am Tag)	... Je öfter, desto besser. Reduziert das Risiko von Datenverlust.
Pricing	Einfache monatliche Abrechnung. All inclusive – einfacher kalkulierbarer Preis pro User.	... keine versteckten Bedingungen, keine komplexen Pricing-Modelle. Volle Kostentransparenz und -kontrolle. Abrechnung einfach über die Anzahl der User. Sharepoints kosten keine Lizenz.
Support	Deutscher Vodafone Expert Support	... ein zentraler Ansprechpartner für die Kund:innen.

Weitere Informationen finden Sie hier:

www.vodafone.de/cloudbackup

Oder kontaktieren Sie uns gerne telefonisch – **kostenfrei** von Montag bis Freitag, **8:00 bis 18:00 Uhr:**

0800 505 45 13

10 Glossar: Cyberbedrohungen, DSGVO und Microsoft 365 Copilot – das steckt hinter den Fachbegriffen

Advanced Persistent Threat

Definition: Ein Advanced Persistent Threat (APT) ist eine besonders ausgeklügelte und über längere Zeit durchgeführte Form eines Cyberangriffs. Dabei infiltrieren gut organisierte, nicht selten staatlich gesteuerte Angreifer gezielt Netzwerke oder Systeme, um über einen längeren Zeitraum hinweg unbemerkt sensible Daten auszuspähen, zu stehlen oder Sabotage zu betreiben. Im Gegensatz zu simpleren Cyberangriffen investieren die Angreifer bei einem APT viel Zeit, Know-how und Ressourcen, um sich dauerhaft Zugang zum Zielsystem zu verschaffen, sich darin zu bewegen und ihre Aktivitäten möglichst lange zu verbergen. Typische Ziele sind Unternehmen, Behörden oder Betreibende kritischer Infrastrukturen.

Botnetz

Definition: Cyberangriffe finden häufig (teil-) automatisiert statt. Zum Einsatz kommen dann Software-„Roboter", kurz „Bots". Wenn mehrere davon in einem Netzwerk zusammenarbeiten (etwa für DDoS-Attacken – Distributed Denial of Service, die gezielte Überlastung von IT-Ressourcen), spricht man von einem „Botnetz".

Computerviren/ Würmer/Trojaner

Definition: Die Analogie von Computerviren zu biologischen Viren soll verdeutlichen, dass sich diese Art von Schadprogrammen selbstständig in den befallenen Systemen und darüber hinaus verbreitet. Der Begriff „Wurm" deutet an, dass sich solche Schadprogramme durch IT-Netzwerke „hindurchfressen". Die Bezeichnung „Trojaner" spielt auf das trojanische Pferd aus der klassischen Sagenwelt an und drückt damit aus, dass der schädliche Inhalt sich oft in einer vermeintlich interessanten oder nützlichen Hülle tarnt. Diese Begriffe sind mittlerweile in den Alltags-Sprachgebrauch eingegangen, und nicht immer ganz trennscharf definiert.

DSGVO

Definition: Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, die seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten gilt und den Schutz personenbezogener Daten natürlicher Personen regelt. Ihr Ziel ist es, einheitliche Standards für die Verarbeitung, Speicherung und Weitergabe personenbezogener Daten zu schaffen, um sowohl die Privatsphäre der Betroffenen zu schützen als auch den freien Datenverkehr im europäischen Binnenmarkt zu gewährleisten. Die DSGVO gilt für Unternehmen, Behörden und Organisationen, die personenbezogene Daten von EU-Bürger:innen verarbeiten. Bei Verstößen gegen ihre Regelungen drohen empfindliche Bußgelder.

Microsoft Copilot

Definition: Microsoft Copilot ist ein KI-gestützter Assistent, der in Microsoft 365 und Windows integriert ist und die Produktivität durch Automatisierung und personalisierte Unterstützung steigert. Zu den wichtigsten Funktionen zählen KI-Unterstützung bei der Erstellung, Zusammenfassung und Analyse von Dokumenten, E-Mails und Präsentationen sowie die Automatisierung von Routineaufgaben wie Terminplanung, Protokollerstellung und Datenverarbeitung. Copilot kann in Echtzeit Gespräche in Microsoft Teams zusammenfassen und Aktionspunkte erfassen. Darüber hinaus ermöglicht Copilot die Entwicklung und Integration von KI-Agenten, die spezifische Geschäftsprozesse automatisieren, etwa im Kund:innen-Service oder bei der Fehlerbehebung.

Ransomware

Definition: Mittlerweile eine der am weitesten verbreiteten Arten von Malware. Ransomware (aus engl. ransom = Lösegeld und Software) verschlüsselt auf dem befallenen System die Nutzerdaten mit einem geheimen Schlüssel. Die Angreifer verlangen vom Angriffsopfer ein Lösegeld, um wieder auf die nicht mehr zugänglichen Daten zugreifen zu können. Sie versprechen, im Gegenzug zur Zahlung den Verschlüsselungscode auszuhändigen – was aber keineswegs immer stattfindet.