

Was das Internet sagt:

Die Nutzung von **SharePoint** und **OneDrive** bringt vor allem Risiken in den Bereichen **Datensicherheit, unkontrollierte Freigaben und Compliance** mit sich.  EDV Systeme Donner +1

Wichtigste Risiken im Überblick

- **Unkontrollierter Datenabfluss (Over-sharing):** Das einfache Erstellen von Freigabelinks (teilweise standardmäßig als anonyme „Jeder“-Links konfiguriert) führt schnell dazu, dass sensible Dokumente ungewollt an Dritte oder im ganzen Unternehmen offengelegt werden.  YouTube · Aaron Siller +1
- **Ransomware und Schadsoftware:** Kompromittierte Benutzerkonten oder infizierte lokale Endgeräte können Schadsoftware direkt über den Sync-Client in die Cloud replizieren und dort Dateien verschlüsseln.  centron +1
- **Täuschender Glaube an ein Backup:** Microsoft bietet zwar Versionierung und Papierkörbe an, dies ersetzt jedoch kein separates, vom Cloud-Tenant unabhängiges Backup gegen versehentliches Löschen durch Admins oder Angreifer.  arian IT Service GmbH
- **Verborgene Berechtigungen und Komplexität:** Durch gewachsene Strukturen, Teams-Kanäle und verschachtelte Ordner verliert man schnell die Übersicht, wer welche Zugriffsrechte besitzt.  Hornetsecurity
- **Datenschutz / DSGVO:** Bei ungeeigneter Konfiguration (z. B. Datenspeicherung oder Einbindung externer Dienste ohne korrekte ADV) drohen Verstöße gegen europäische Datenschutzvorgaben.

◆ Übersicht mit KI

Die größten Risiken bei der Nutzung von SharePoint Online liegen in **unkontrollierten Freigabelinks, fehlenden Governance-Richtlinien und dem unbemerkten Abfluss oder Verlust sensibler Daten durch falsche Berechtigungen**. 

Hier sind die wichtigsten Risiken im Detail:

1. Unsichere Standardeinstellungen und Freigaben

- **Offene Links:** Die Werkzeugeinstellungen von Microsoft 365 erlauben oft, dass Dateien per Link an anonyme Personen oder externe Dritte weitergegeben werden.  Hornetsecurity
- **Unübersichtliche Rechte:** Wenn viele Teams und Ordner erstellt werden, verlieren Administratoren schnell den Überblick darüber, wer welche Zugriffsrechte besitzt.  Hornetsecurity

2. Datenschutz und Compliance (DSGVO)

- **Personenbezogene Daten:** Werden Kundendaten oder Mitarbeiterdaten unverschlüsselt oder frei zugänglich gespeichert, drohen Verstöße gegen die Datenschutz-Grundverordnung (DSGVO).
- **Meldepflicht:** Ein unberechtigter Zugriff von außen oder innen gilt schnell als meldepflichtiger Datenschutzvorfall.  Gröpper IT-Systemtechni...

3. Datenverlust und Ransomware

- **Schadsoftware:** Verschlüsselungs-Trojaner (Ransomware) können Dateien im Cloud-Speicher infizieren oder unbrauchbar machen, wenn Konten von Mitarbeitern übernommen werden.  Gröpper IT-Systemtechni...
- **Irrtum:** Versehentliches Löschen durch Nutzer kann zwar über den Papierkorb abgefedert werden, ersetzt jedoch keine professionelle, externe Backup-Strategie.

4. Fehlende Governance und Wildwuchs

- **Chaos in der Struktur:** Ohne klare Regeln für die Erstellung von SharePoint-Seiten entsteht ein unkontrollierter Wildwuchs (Sprawl).
- **Sicherheitslücken durch Unwissenheit:** Aktuelle Berichte, wie die von [heise online](#) zu Sicherheitslücken, zeigen, dass auch Cloud-Infrastrukturen stets überwacht und richtig konfiguriert sein müssen.  Heise Online +1



IONOS

https://www.ionos.de > ... > Hosting > Hosting-Technik



Diese Website ist sicher.

Was ist Cloud Hosting? | Die Vor- und Nachteile

20.05.2025 — Beim **Cloud**-Hosting handelt es sich um ein Webhosting-Modell mit frei skalierbaren Serverressourcen und einer maximalen Kostentransparenz.

Weitere Fragen

Welche 3 Nachteile hat die Cloud?



Übersicht mit KI

Die drei größten Nachteile der Cloud sind die **Abhängigkeit von einer Internetverbindung, Sicherheits- und Datenschutzbedenken sowie die laufenden Kosten**. Alexander Thamm [at] +1

Die 3 Nachteile im Detail

- **Internetabhängigkeit:** Ohne eine stabile und schnelle Internetverbindung ist der Zugriff auf Daten und Anwendungen in der Cloud nicht möglich. Fällt das Netz aus, steht die Arbeit still. MaibornWolff GmbH +2
- **Sicherheit und Datenschutz:** Da die Daten auf externen Servern eines Drittanbieters liegen, gibt man die direkte Kontrolle über die physische Sicherheit aus der Hand. Es besteht das Risiko von Cyberangriffen auf den Anbieter oder unklaren rechtlichen Vorgaben beim Datenschutz. YouTube · U-Labs +3
- **Laufende Kosten:** Cloud-Dienste werden meist über Abos oder nach tatsächlicher Nutzung bezahlt. Auf Dauer können diese monatlichen Ausgaben höher sein als der einmalige Kauf eigener Hardware. DATA MART Consulting +1

Können Daten in der Cloud verloren gehen?



✦ Übersicht mit KI

Ja, Daten in der Cloud können verloren gehen, auch wenn die Speicherplätze von großen Anbietern technisch gut gesichert sind. Datenrettung Swiss

Häufige Ursachen für Datenverlust in der Cloud

- **Menschliche Fehler:** Dateien werden versehentlich gelöscht oder überschrieben. Oft ist der Papierkorb nur für begrenzte Zeit (zum Beispiel 30 Tage) verfügbar. Keys.Express +1
- **Synchronisationsfehler:** Ein Fehler auf einem Gerät wird automatisch mit der Cloud abgeglichen, wodurch gute Daten durch fehlerhafte ersetzt werden. KUERT Datenrettung +1
- **Schadsoftware (Ransomware):** Verschlüsselt ein Virus Dateien auf Ihrem Computer, lädt die Synchronisation diese kaputten Dateien oft direkt in die Cloud hoch. NXT-IT +1
- **Ablauf des Kontos:** Wenn Abonnements ablaufen oder Zahlungsdaten ungültig werden, kann der Zugang zum Speicher verloren gehen. Datenrettung Germany
- **Haftung der Anbieter:** Wie in den [Apple iCloud-Bedingungen](#) nachzulesen ist, übernehmen viele Anbieter keine absolute Garantie gegen Datenverlust und empfehlen eigene Sicherheitskopien.

Wichtig zu wissen

Eine Cloud ist **kein echtes Backup**. Ein Cloud-Dienst spiegelt meist nur den aktuellen Zustand Ihrer Dateien. Wenn eine Datei gelöscht wird, ist sie meist überall weg. Speichern Sie wichtige Daten zusätzlich lokal oder auf einer externen Festplatte ab. mit.data

✦ Übersicht mit KI

Bei der Nutzung von Microsoft OneDrive bestehen vor allem **Risiken beim Datenschutz, durch fehlende Ende-zu-Ende-Verschlüsselung und bei der automatischen Synchronisierung**.  YouTube · Jakob Neuba... +2

 Datenschutz und US-Recht (Cloud Act)

- **Fehlende End-to-End-Verschlüsselung:** Microsoft speichert die Schlüssel selbst.
- **Zugriff durch Behörden:** Der US CLOUD Act verpflichtet Microsoft zur Datenherausgabe an US-Behörden.
- **Datenschutz (DSGVO):** Sensible Daten erfordern strenge Zusatzvereinbarungen und bergen rechtliche Hürden.  IONOS +3

 Automatische Synchronisierung und Datenverlust

- **Verschiebung statt Backup:** Die Funktion „Desktop, Dokumente, Bilder sichern“ kann lokale Ordner in die Cloud verschieben.
- **Synchronisationsfehler:** Bei Löschung auf einem Gerät werden Dateien oft überall gelöscht.
- **Ransomware-Gefahr:** Infiziert Schadsoftware den lokalen PC, syncnt OneDrive die verschlüsselten Dateien direkt in die Cloud.  YouTube · Jakob Neubauer

 Zugriff und Kontosicherheit

- **Passwortverlust:** Ist das Microsoft-Konto gesperrt oder gehackt, droht der Totalverlust des Zugriffs.