

Cloud Computing – Datenspeicherung im Internet



HAND-
REICHUNG
#9

www.digital-kompass.de

Herausgeber:



**Deutschland
sicher im Netz**

Mit Unterstützung von:



Gefördert durch:



Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

Herausgeber:

Digital-Kompass
c/o Deutschland sicher im Netz e.V.
Albrechtstraße 10 c
10117 Berlin
info@digital-kompass.de
www.digital-kompass.de

V.i.S.d.P.:

Dr. Michael Littger

Redaktion:

Daniel Lehmann

Gestaltung und Satz:

alles mit MEDIEN
www.allesmitmedien.de

Druckerei:

WIRmachenDRUCK GmbH
www.wir-machen-druck.de

Erscheinungsjahr:

1. Auflage 2019

Titelbild:

© ArtFamily – stock.adobe.com

Cloud Computing

Einleitung	5
1. Was ist eine Cloud?	6
2. Wie man von der Cloud profitieren kann	8
3. Welche Anwendungsmöglichkeiten gibt es?	9
4. Tipps für das effiziente Arbeiten in der Cloud	22
5. Was bei der Cloud-Nutzung zu berücksichtigen ist	23
6. Wie schütze ich meine Daten in der Cloud?	25
Glossar	36
Quiz	40

Liebe Leserinnen und liebe Leser,

das Internet bietet eine Fülle von Chancen, unseren Alltag zu erleichtern. Das gilt in besonderem Maße für ältere Generationen. Dafür setzen wir auf Ehrenamtliche wie Sie, die ältere Menschen über den sicheren Umgang mit dem Internet aufklären. An Sie wenden wir uns mit dem *Digital-Kompass*.

Der *Digital-Kompass* umfasst Angebote, die Sie in Ihrem Engagement unterstützen. Die vorliegende Reihe von Handreichungen gehört dazu: mit kompakten Informationen und praktischen Übungsaufgaben, die Sie in Ihrer täglichen Arbeit mit Senioren verwenden können. Weitere Dokumente finden Sie in der *Material-Fundgrube*.

In unseren *Digitalen Stammtischen* laden wir Sie außerdem ein, online mit Experten und Gleichgesinnten über aktuelle Fragen rund ums Internet zu sprechen.

Unsere Angebote finden Sie auch bei *Digital-Kompass Standorten* in Ihrer Region.

Der *Digital-Kompass* ist ein Verbundprojekt von Deutschland sicher im Netz e.V. und der Bundesarbeitsgemeinschaft der Senioren-Organisationen mit Förderung des Bundesministeriums der Justiz und für Verbraucherschutz – in Partnerschaft mit der Verbraucher Initiative e.V.

Besuchen Sie uns unter www.digital-kompass.de.

Viel Vergnügen beim Lesen!

Ihr
Dr. Michael Littger
Geschäftsführer
Deutschland sicher im Netz e.V.

Ihr
Joachim Schulte
Projektleiter Digital-Kompass
Deutschland sicher im Netz e.V.

Einleitung

Es ist erstaunlich, wie schnell sich die Technik innerhalb weniger Jahre weiterentwickelt hat und wie umfassend die Digitalisierung mittlerweile Einfluss auf alle Lebensbereiche ausübt – vor allem auf die Bereiche der Kommunikation und des Informationsaustauschs. Wollte man früher etwa Bilder vom gemeinsamen Urlaub an alle Beteiligten weitergeben, mussten erst die Filme entwickelt, Abzüge erstellt und diese dann an alle übergeben werden.

Heutzutage geht das viel einfacher – zum Beispiel mit Cloud Computing. Der Begriff kommt aus dem Englischen und bedeutet Daten- oder Rechnerwolke. Er beschreibt die Verwendung von IT-Infrastrukturen, die über ein Rechnernetz miteinander verbunden sind. Cloud-Computing-Dienste verschiedenster Art ermöglichen unter anderem die zeit- und ortsunabhängige Nutzung von Speicherplatz und den Zugriff auf Computerprogramme – von der Pflege eines Team-Kalenders über die Freigabe von in der Cloud gelagerten Foto-Galerien an Familie und Freunde bis hin zur zeitgleichen Korrektur eines Textes. Trotzdem gaben in der Befragung „Digitale Nutzung in Deutschland 2018“ des Bundesverbands Digitale Wirtschaft (BVDW) lediglich 48 Prozent der befragten Nutzerinnen und Nutzer an, Cloud-Dienste zu nutzen.

In dieser Handreichung geben wir Ihnen einen Einblick in die unterschiedlichen Formen von Cloud Computing und veranschaulichen deren Funktionsweisen. In der Folge

stellen wir Ihnen mögliche Anwendungsfelder für private wie berufliche oder ehrenamtliche Zwecke vor. Damit die Arbeit mit der Cloud reibungslos abläuft, geben wir Tipps, wie Daten und Dateien richtig gespeichert und bearbeitet werden – insbesondere dann, wenn mehrere Personen beteiligt sind. Einen wichtigen Aspekt stellt zudem der Datenschutz dar: Wir erklären, welche Maßnahmen Sie selbst treffen können, damit Ihre persönlichen Inhalte nicht in falsche Hände geraten oder verloren gehen und beleuchten, worauf Sie ansonsten achten müssen.

1. Was ist eine Cloud?

Cloud-Computing umfasst sowohl die Nutzung als auch das Anbieten unterschiedlicher IT-Dienstleistungen (Server, Speicher, Datenbanken, Netzwerkkomponenten, Software, Analyse-Funktionen) über ein Netzwerk. Statt Dateien oder Anwendungen lokal auf dem eigenen Gerät zu speichern, greift man über ein Programm (auch Client genannt) oder einen Webbrowser darauf zu. Zugangsgeräte können daher von Desktop-PCs, Laptops, Smartphones über Tablets bis hin zu Wearables (tragbare Computersysteme wie „intelligente“ Uhren oder Datenbrillen) alle internetfähigen Elemente sein. Das Internet, beziehungsweise ein nicht öffentliches Intranet, ist ebenso notwendige Grundlage wie eine schnelle Breitbandverbindung, um die gewünschten Inhalte von externen Servern zügig laden zu können.

Dabei unterscheidet man zwischen drei sogenannten Servicemodellen:

Nutzt man ganze Anwendungsprogramme eines Anbieters, wie zum Beispiel die *Microsoft Office Cloud*, als Dienstleistung, wird dies als Software bei Bedarf (im Englischen Software as a Service → SaaS) bezeichnet. Die Ihnen vorliegende Handreichung befasst sich in der Folge vor allem mit diesem Modell.

Wer IT-Systeme für die Datenverarbeitung, den Datentransport und die Datenspeicherung bei beliebigen Prozessen benötigt, kann die erforderlichen Komponenten beziehungsweise die komplette Infrastruktur inklusive Wartung, mieten (Infrastructure as a Service → IaaS). Das können Server, Rechnernetze und Datenbanken sein.

Eher für Entwickler interessant ist das zweite Modell: Plattform bei Bedarf (Platform as a Service → PaaS). Hier können eigene Anwendungen erschaffen, getestet und ausgeliefert werden, ohne selbst in die dafür notwendige Hardware und Software investieren zu müssen.

Zusätzlich wird über vier sogenannte Liefermodelle die Zugangsmöglichkeit beschrieben: Eine „öffentliche Rechnerwolke“ (Public Cloud) kann grundsätzlich von allen genutzt werden. Im Gegensatz dazu steht die „private Rechnerwolke“ (Private Cloud), die von einem Unternehmen oder einer Organisation allein installiert und betrieben wird. Die Mischform aus beiden Varianten wird Hybrid Cloud genannt. Für manche Gemeinden, öffentliche Ämter, Bildungseinrichtungen oder andere Gesellschaften und Kooperationen mit

ähnlichen Interessen kann eine Community Cloud sinnvoll sein. Sie funktioniert genau so wie eine öffentliche Rechnerwolke – mit dem Unterschied, dass die Kosten auf mehrere Parteien verteilt werden und eine gemeinschaftliche Nutzung erfolgt.

2. Wie man von der Cloud profitieren kann

Eine Rechnerwolke, im Folgenden auch Cloud genannt, bietet sowohl für Privatpersonen als auch für Unternehmen eine ganze Reihe von Vorteilen. An dieser Stelle soll es um Einzelanwender gehen. Vor allem benötigen Sie keine eigene Hard- und Software, um Cloudanwendungen zu nutzen. Vorbei sind die Zeiten, in denen die Festplatte des Computers vorgab, wie viele Daten und Anwendungen gleichzeitig gespeichert und installiert sein konnten. So sind auch Speicherlösungen wie USB-Sticks oder externe Festplatten als Datenträger zunehmend überholt, die anfällig für Beschädigungen oder Verlust sind.

In der Cloud kann der Zugriff jederzeit von verschiedenen Geräten aus geschehen. Oder man teilt die Daten gleich mit Freunden, Familie oder Arbeitskollegen, tauscht sie aus und bearbeitet sie – ohne am selben Ort sein zu müssen. Da der Cloud-Anbieter die Wartung übernimmt und damit gewährleistet, dass alles funktioniert, bleibt das eigene System auf Dauer unberührt. Ein dauerhaftes Nachrüsten des Rechners ist somit nicht notwendig.

Die einzigen Voraussetzungen bleiben ein aktiver Internetzugang und ein Zugang zur Dienstleistung. Das kann ein Webbrowser sein oder, wenn verfügbar, die zum Cloud-Angebot passende App oder Desktop-Anwendung.



Daten in der Rechnerwolke

3. Welche Anwendungsmöglichkeiten gibt es?

Cloud-Dienstleistungen können in der Summe zunächst all das leisten, was herkömmliche Hard- und Software-Lösungen auf Computern auch bewerkstelligen können: von der simplen Datenspeicherung über Mittel zur Arbeitsorganisation bis hin zu Office-Anwendungen. Eine Begrenzung gibt es theoretisch nicht. Im Grunde kann alles, was über einen

Rechner geschieht, genauso gut in die Cloud ausgelagert werden. Dies wird auch durch die weiter steigende Zahl an Diensten deutlich, die in allen Bereichen stetig dazukommen. Die beliebtesten stellen wir Ihnen in den folgenden Kapiteln vor. Das US-Forschungs- und Beratungsunternehmen *Gartner Inc.* hat in einer Erhebung im September 2018 den weltweiten Umsatz mit Cloud-Software (SaaS) ermittelt. Im Jahr 2017 belief sich dieser auf 59 Milliarden US-Dollar. Bis 2021 soll sich der Wert fast verdoppeln und auf über 113 Milliarden ansteigen. Nachfolgend stellen wir Ihnen typische Einsatzbereiche und die prominentesten Vertreter in diesen Gebieten vor.

Die Cloud als Datenspeicher und Backupdienst

Statt den eigenen Systemspeicher zu belasten oder externe Datenträger zu verwenden, setzen Nutzerinnen und Nutzer zunehmend auf Cloud-Speicher. Ob Musik, Fotos oder Dokumente: Über solche Dienste kann man über ein passwortgeschütztes Nutzerkonto jederzeit von jedem Ort darauf zugreifen, solange eine Internetverbindung besteht. Messenger-Dienste wie *WhatsApp* bieten überdies Backup-Lösungen für Chats bei bestimmten Cloud-Anbietern an – in dem Fall *Google Drive* und *iCloud*. Ein Backup (zu Deutsch: Datensicherung) ermöglicht bei Datenverlust die Wiederherstellung eines zum Speicherzeitpunkt vorherrschenden Zustands.



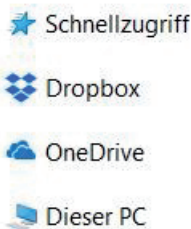
Achtung:

Auch in der Cloud gilt das Urheberrecht! Fremde Inhalte (Musik, Fotos, Texte) dürfen Sie nur hochladen, wenn Sie die Erlaubnis der Rechteinhaber haben. Privatkopien sind grundsätzlich zwar ebenfalls gestattet, wenn nur Sie selbst darauf zugreifen. Schwierig wird in einem Streitfall die Abgrenzung des privaten Rahmens allerdings, wenn auch der Familien- und Freundeskreis den Zugriff erhält.

Momentan dürften nach wie vor *Google Drive* (weltweit über eine Milliarde Nutzer, Stand 2018), *Dropbox* (500 Millionen Nutzer, Stand 2016) und *Microsoft One-Drive* (500 Millionen Nutzer, Stand 2017) zu den größten Anbietern gehören. In der Grundfunktionalität unterscheiden sie sich nur geringfügig. Über den Browser, einen Desktop-Client (eine Software, die auf dem eigenen Rechner installiert wird, um direkt auf die Cloud zuzugreifen) oder die Smartphone-App verwaltet die Nutzerin bzw. der Nutzer die Daten in der Ordnerstruktur, wie sie auch zum Beispiel beim Betriebssystem Windows genutzt wird. Sie können beliebig oft hoch- oder heruntergeladen, verschoben oder umbenannt werden. Bei Bedarf können Dateien und Ordner angelegt oder zugewiesen werden, auf die mehrere Personen Zugriff bekommen, beispielsweise bei einer Projektarbeit oder für den Austausch von Bildern nach einer Hochzeit.

Bei der Verwendung eines Clients wird der Online-Speicher in den System-Speicher integriert und verbraucht die

entsprechenden Ressourcen. Es wird also ein genaues Abbild der Datenstruktur aus der Cloud auf Ihrer Festplatte gespeichert. Dafür stehen Ihnen die Daten über dieses Gerät auch offline zur Verfügung. Sämtliche Aktionen, die sie in diesem Laufwerk ausführen, werden bei bestehender Internetverbindung und aktivem Client mit dem Online-Speicher synchronisiert. Alles, was sie dort kopieren, verschieben, anlegen und löschen wird sofort entsprechend in der Cloud umgesetzt.



Die Clients von Dropbox und OneDrive als integrierte Bestandteile des Windows Explorers

Unterschiede bei den Cloudspeicher-Angeboten bestehen vor allem bei dem zur Verfügung gestellten Speicherplatz und den Tarifen. Während beispielsweise *Dropbox* in der Basis-Version lediglich 2 Gigabyte (abgekürzt: GB) anbietet, sind es bei *Google Drive* schon 15 GB.¹ Bevor Sie sich für einen Dienst entscheiden, sollten Sie allerdings mehrere Faktoren berücksichtigen.

¹ Stand August 2019

So ist *Microsoft OneDrive* unter anderem deshalb erfolgreich, weil der Speicherdienst sehr eng mit dem hauseigenen Betriebssystem *Windows 10* verknüpft ist. *Google Drive* überzeugt durch die Verzahnung mit weiteren *Google Services* wie *Gmail* und *Fotos* – um die man allerdings auch nicht herum kommt, da ein vorhandenes *Google-Konto* Voraussetzung ist. Wer das möchte, kann die mit dem Smartphone aufgenommenen Bilder direkt in der Cloud speichern lassen oder Anhänge aus E-Mails dorthin verlagern.

Als „öffentlich“ markiert hochgeladene Inhalte sind über die Suchmaschine von *Google* auffindbar. Seit November 2018 gibt es auch in Deutschland bei *Google One* neue Tarife für ein Cloudspeicher-Abonnement, das über die 15 GB gratis hinausgeht.



Verfügbarer Speicherplatz in Google Drive

Wer einen Anbieter sucht, der die persönlichen Daten auf Servern in Deutschland speichert, wird beispielsweise in der *MagentaCLOUD* der *Telekom* fündig. Hier erhält man zunächst 10 GB kostenlosen Speicherplatz. Man muss kein *Telekom*-Kunde sein, um den Dienst nutzen zu können.

Für Nutzer der Freemail-Anbieter *GMX* oder *Web.de* stehen ebenfalls Cloud-Speicher zur Verfügung. Bei beiden startet man mit derzeit mit 2 GB Speicherplatz. Weitere Services mit deutschem Serverstandort sind zum Beispiel *DriveOnWeb*, *HiDrive*, *MyTuxedo* oder auch die *E-Post Cloud*.

Unter Umständen ist es sinnvoll, wenn Sie mehrere Cloud-Anbieter miteinander kombinieren, um Ihr Dateimanagement zu optimieren. Ratsam ist es auf jeden Fall grob zu schätzen, welche und wie viele Daten Sie speichern möchten. In eine Cloud mit 2 GB Speicherplatz passen beispielsweise rund 600 Songs oder 700 Bilder. Word-Dokumente hingegen sind weitaus weniger speicherintensiv: Davon würden ungefähr 100.000 Seiten auf diesen Speicherplatz passen.



Aufgabe

Erstellen Sie eine Tabelle mit allen Daten-Typen (Foto, Video, Text) und Ordnern, die Sie speichern wollen, mit ihrem jeweiligen Datenvolumen. Notieren Sie in einer extra Spalte den dafür erforderlichen Cloudspeicher.

Checkliste für die Wahl des richtigen Anbieters



1. Welche Daten möchte ich in der Cloud speichern?
2. Wie viel Speicherplatz brauche ich dafür?
3. Bin ich bereit Geld dafür auszugeben?
4. Ist mir der Serverstandort wichtig?
5. Wie oft werde ich voraussichtlich auf die Cloud zugreifen?
6. Brauche ich einen Client und/oder eine Smartphone-App?
7. Möchte ich Dateien gemeinsam mit anderen bearbeiten?
8. Nutze ich bereits einen Dienst, der auch einen Cloud-Speicher anbietet (GMX, Web.de, Telekom, Amazon, Google)?
9. Nutze ich ein Apple-, Windows-, oder Google-Gerät?

Die Cloud als Zusammenarbeits-Werkzeug



Simultanes Arbeiten in der Cloud

Der gleichzeitige Zugriff auf ein und dasselbe Dokument von verschiedenen Computern aus wird oft „gemeinsame Dokumenterstellung“ oder „Zusammenarbeit in Echtzeit“ genannt. Anbieter und Produkte in diesem Bereich sind unter anderem *Office 365* und *Google Docs*. Mit beiden wird vermieden, dass unterschiedliche Varianten einer Datei mühsam zwischen allen Beteiligten immer wieder verschickt werden müssen und Versionskonflikte entstehen. Wenn beispielsweise verschiedene Personen unterschiedliche Passagen zu einem Text beisteuern, müssen diese nicht erst gesammelt, überarbeitet und zusammengefügt werden.

Stattdessen können alle übersichtlich in demselben Dokument arbeiten, Änderungen sofort nachvollziehen und sich direkt über Kommentare oder sogar einen eigenen Chat austauschen. Das funktioniert mit Word-Formaten ebenso wie mit Präsentationen und Tabellen. In der Regel werden über kleine Avatare (grafische Figuren, die einer Nutzerin oder einem Nutzer zugeordnet werden) und verschiedenfarbige Icons und Mauszeiger angezeigt, wer gerade ebenfalls die Datei geöffnet hat. Je nach Freigabeoptionen und -einstellungen kann der- oder diejenige nun mit allen Rechten darin arbeiten, Inhalte ergänzen, löschen oder speichern.

Alternativ gibt es noch die Möglichkeit, von Dritten lediglich Kommentare zuzulassen oder ihnen nur die schreibgeschützte Ansicht (read only) zukommen zu lassen. Die Freigabe kann gezielt an eine oder mehrere Kontakte und deren E-Mail-Adressen gehen oder allgemein als Link verbreitet werden. Die erstgenannte Variante ist dabei die sicherere, da sich darüber kontaktierte Personen für gewöhnlich mit ihren Nutzerdaten beim Dienst anmelden müssen. Eine Linkfreigabe hingegen führt meist direkt zum Dokument. Gerät diese in die falschen Hände, sind womöglich sensible Inhalte sofort sichtbar. Zumal eine Einladung nicht beliebig weitergeleitet werden kann, ein Link allerdings schon.

Manche Dienste bieten in Form von Browser-Erweiterungen (Add-ons oder Plug-ins) die Möglichkeit Dateien auch offline zu bearbeiten. Sobald dann wieder eine Internetverbindung hergestellt wurde, werden die vollzogenen Änderungen online für alle sichtbar gespeichert. Die meisten

Anbieter verfügen über eine Art „Versionskontrolle“: Mit wenigen Klicks lässt sich eine Datei in den Zustand früherer Bearbeitungsstände zurückversetzen. Dabei werden sämtliche Abweichungen farblich festgehalten und den Personen zugeordnet, die die Datei bearbeitet haben.

Versionsverlauf
Nur benannte Versionen anzeigen ☒
LETZTE WOCHE
3. Juli, 09:55 ⋮ Aktuelle Version ● Daniel Lehmann
APRIL
27. April, 13:43 ● Alle anonymen Nutzer
▶ 25. April, 22:44 ● Daniel Lehmann

Versionsverlauf einer Datei in Google Drive

Die Cloud als Planungs- und Organisationsinstrument

Gerade bei größeren Gruppen ist es mitunter schwierig einen für alle passenden Termin zu finden. Auch dabei können Cloud-Anwendungen helfen. Online-Dienste wie *Doodle* oder *Kulibri* erlauben es beliebig viele Vorschläge in einer Art Umfrage an einen Teilnehmerkreis zu schicken. Sind sämtliche Antworten eingegangen, wird farblich für alle ersichtlich hervorgehoben, wer wann kann und welcher Tag oder welche Uhrzeit für die Mehrheit möglich ist.

Doch nicht nur einzelne Ereignisse lassen sich so gemeinsam planen. Im Netz lässt sich auch eine Vielzahl an anpassbaren Kalendern finden, die Sie für bestimmte Zwecke und Zugriffe definieren können. Möchten Sie beispielsweise jemanden jederzeit wissen lassen, wann Sie welche Verpflichtungen haben, geben Sie beispielsweise Ihren „Arbeits“-Kalender frei – und umgehen so, dass auch Ihre privaten Vorhaben, die Sie in demselben Dienst unter „Freizeit“ als separaten Kalender gespeichert haben, einsehbar sind. Bei gemeinsamen Terminen können Sie oft bestimmte Dokumente, wie zum Beispiel die Online-Tickets, gleich anhängen. Oder Sie lassen wie bei *Google Kalender* Ihre Termine aus *Gmail* direkt eintragen.

Eine Projektmanagementsoftware wie *Trello*, *Airtable* oder *Asana* verknüpft viele solcher Funktionen. Entscheidende Vorteile sind wieder der simultane Austausch und der zeit- wie ortsunabhängige Abruf von Informationen. Über *Trello* lassen sich einfach Redaktionspläne, Organisationsabläufe und aufbereitete Daten anlegen – und gegebenenfalls sogar mit Inhalten aus Cloudspeicher-Diensten verknüpfen.

Die Cloud als Kommunikationsmittel

Cloud-Mail-Dienste sind streng genommen keine technische Neuheit der letzten Jahre, da jede Web-Mail, die man ohne eigenen Server genutzt hat, schon seit jeher die Kriterien einer Mail aus der Cloud erfüllt. Hinzugekommen sind jedoch neue Dienste und eine verbesserte Verschlüsselung der Daten in der Cloud. Deutsche Anbieter wie *Posteo* oder

Mailbox.org legen dabei besonderen Wert auf Datenschutz und Datensicherheit. Außerdem sind sie bewusst werbefrei gehalten. Beide Dienste erheben keine persönlichen Daten, weshalb eine anonyme Nutzung möglich ist. Der Zugriff über die Server erfolgt grundsätzlich über verschlüsselte TLS-Verbindungen. TLS steht für Transport Layer Security, was so viel wie Transportschichtsicherheit bedeutet und ein Verschlüsselungsprotokoll bei der Datenübertragung darstellt. Zudem wird verhindert, dass eventuell gespeicherte Verbindungsdaten von Dritten im Nachhinein entschlüsselt werden können.

Neben Mails sind aber auch alle anderen online-basierten Kommunikationsformen über eine Cloud möglich. Von Instant-Messaging-Diensten über gemeinsame Texteditoren (Etherpads) bis hin zur Cloud-Telefonie.

Die Cloud als Programmspeicher

Früher musste Software im Laden erworben oder im Internet heruntergeladen werden. Danach folgte die Installation auf dem Gerät. Als Nutzer musste man deshalb gleich mehrere Punkte beachten: Der benötigte Speicherplatz des Programms im System, die Kompatibilität zum genutzten Betriebssystem (typischer Fehler: Anwendungen für Windows mit 32-Bit oder 64-Bit verwenden wollen, obwohl genau die andere Version auf dem Rechner läuft), die Leistungsfähigkeit des Prozessors (CPU), der Grafikkarte oder des Arbeitsspeichers (RAM) und andere Dinge wie bestimmte Eingabegeräte.

Doch selbst wenn die Mindestanforderungen erfüllt sind, bedeutet das nicht, dass die gewünschte Anwendung störungsfrei und leistungsstark läuft. Ein Computer ist ein komplexes Konstrukt aus vielen ineinander verzahnten Komponenten, bei dem mitunter bereits eine kleine Veränderung dafür sorgt, dass ein Programm nicht mehr richtig ausgeführt werden kann. Hinzu kommen etwaige Updates, die vorgenommen werden müssen, um die Software aktuell zu halten oder auch um Sicherheitsrisiken zu begegnen.

All das ist bei Programmen aus der Cloud kein Thema. Wie bei den bisher vorgestellten Anwendungsmöglichkeiten auch, laufen Cloud-Programme über den Webbrowser (obwohl viele Anbieter inzwischen zusätzlich eine Desktop-Version anbieten). Oft handelt es sich bei ihnen um abgespeckte Varianten einer Kauf-Software, die dafür auf fast allen Geräten verwendet werden kann. Dies ist zum Beispiel bei *Photoshop Express* von *Adobe* der Fall. Für Büro-Anwendungen stehen für jedes internetfähige Gerät mit Webbrowser beispielsweise *Google Docs* oder *Microsofts Office 365* zur Verfügung. Die Anwendungen werden vom Anbieter immer auf dem neuesten Stand gehalten, der Nutzer muss selbst nicht tätig werden. Eine Sonderform stellt das Cloud Gaming dar: Hierbei werden Videospiele auf einem Server ausgeführt, die Nutzereingaben werden an diesen gesendet. Ausgegeben werden dann die Audio- und Video-Elemente.

**Achtung:**

Anders als bei dem analogen Erwerb von Programmen (sogenannte Boxkäufe) werden viele Anwendungen, die Sie über eine Cloud nutzen, über ein Abonnement abgerechnet. Behalten Sie jederzeit den Überblick, wie viele zahlungspflichtige Dienste Sie verwenden und wie die Zahlungsmodalitäten und -intervalle aussehen. Überlegen Sie, wie lange Sie die Software voraussichtlich nutzen und wie oft sie aktualisiert werden muss. Wägen Sie dann ab, ob sich ein Einmal-kauf oder ein Cloud-Abo für Sie lohnt.

4. Tipps für das effiziente Arbeiten in der Cloud

Das gemeinsame Planen, Erstellen und Bearbeiten von Dokumenten in einer Cloud kann viele Arbeitsprozesse erleichtern. Doch um das volle Potential solcher Dienste und Plattformen wirklich auszuschöpfen und unnötige Hindernisse zu vermeiden, sollten je nach Anwendung folgende Hinweise berücksichtigt werden:

- Überlegen Sie sich eine sinnvolle, übersichtliche und möglichst langfristig angelegte Ordner-Struktur.
- Behalten Sie stets den Überblick darüber, wer Zugang zu welchen Dateien in Ihrer Cloud hat – und welche Bearbeitungsrechte zugewiesen wurden (beispielsweise „nur

ansehen“). Personen, die nicht mehr an einem Projekt beteiligt sind, sollten besser wieder entfernt werden.

- Stoppen Sie die Synchronisierung Ihres Cloud-Clients, wenn Sie Ihre Internetverbindung gerade für andere Zwecke benötigen. Die meisten Anbieter geben Ihnen die Möglichkeit die Download- und Upload-Geschwindigkeit selbst zu regulieren. Über eine sogenannte selektive Synchronisierung können Sie zudem ganze Ordner von der Synchronisierung ausschließen.
- Geben Sie Dokumenten und Dateien aussagekräftige Titel, damit Sie selbst und andere sie leichter finden und zuordnen können. Arbeiten Sie mit Datei-Formaten, die auch andere öffnen und bearbeiten können, ohne beispielsweise in der Textverarbeitung ungewollt das Layout zu beeinflussen.

5. Was bei der Cloud-Nutzung zu berücksichtigen ist

So praktisch eine Cloud an vielen Stellen ist, so hat sie doch auch ihre Restriktionen. Zunächst genannt werden sollte die Abhängigkeit von einer stabilen Internetverbindung mit einer gewissen Bandbreite. Ohne diese lassen sich die meisten Cloud-Programme gar nicht erst ausführen. Zwar gibt es für manche bereits Browsererweiterungen, die eine Offline-

Bearbeitung ermöglichen, allerdings ist dann immer noch nicht die aktuelle Version einer Datei auf allen genutzten Geräten abrufbar. Wenn Inhalte eines Cloud-Speichers nicht lokal (beispielsweise über einen Client) gespeichert sind, ist ein Zugriff schlicht nicht möglich.

Je nach Art, Größe und Umfang eines Projekts und des Nutzungsgrads einer Cloud-Anwendung machen Sie sich unter Umständen abhängig von einem Anbieter. In der Wirtschaftswissenschaft nennt man das den Lock-in-Effekt (englisch *to lock in*: einschließen oder einsperren). Folgende Fragen sollten deshalb vor der Nutzung eines Dienstes mitbedacht werden: Was passiert, wenn der gewünschte Anbieter seinen Service einstellt oder die Tarife ändert? Wie kompatibel sind bestimmte Dateiformate? Wie leicht ist ein Wechsel zu einem vergleichbaren Dienst realisierbar?

Nicht unterschätzt werden sollte der Sicherheitsaspekt. Im Englischen kursiert der ironische Spruch „There is no cloud, it's just someone else's computer“ (Es gibt keine Rechnerwolke, es gibt nur den Computer eines anderen) – was im Grunde das Prinzip der Cloud beschreibt. Aber es macht auch deutlich, dass Daten und Informationen nicht mehr nur in der eigenen Hand liegen. Alles, was wir irgendwo hochladen, erstellen und bearbeiten, ist unter Umständen über die Administratoren des Angebots abruf- und auslesbar – oder bietet einfach einen weiteren Einstiegspunkt für Dritte, der entsprechend geschützt werden muss. Um Datensicherheit und Zugriffsrechte soll es in den folgenden Kapiteln deshalb ausführlicher gehen.

6. Wie schütze ich meine Daten in der Cloud?

So viele Vorteile die Nutzung von Cloud-Computing-Diensten auch bieten, so steht doch eines fest: Wie auch alle anderen Inhalte im Netz können dort hinterlegte Daten oder Dateien das Ziel von Cyberattacken sein oder über Sicherheitslecks gefährdet werden (beispielsweise können Passwörter verloren gehen oder Kundeninformationen für Unbefugte einsehbar sein). Persönliche Daten in eine Cloud hochzuladen, erfordert großes Vertrauen. Eine absolut sichere Cloud existiert noch nicht, aber viele Anbieter bemühen sich verstärkt um eine erhöhte Sicherheit. Nutzerinnen und Nutzer stehen deshalb vor allem vor folgenden Risiken:

- Identitätsdiebstahl – das heißt, dass sich jemand anderes als Ihre Person ausgibt
- Sicherheitsrisiken bei den Endgeräten, die auf die Cloud-Dienste zugreifen (Smartphone, Laptop, PC)
- Datenverlust beziehungsweise Datenmissbrauch

Um dem vorzubeugen oder zumindest entgegenzuwirken, sollten Sie vor der Verwendung der entsprechenden Dienste bereits eine klare Vorstellung für die Nutzung haben. Zentrale Fragen sollten an dieser Stelle lauten:

- Welchen Zweck soll der Dienst konkret erfüllen?
- Welche Alternativen mit einem zumindest ähnlichen Leistungsumfang gibt es?
- Welche personenbezogenen oder sensiblen Daten sind für die Nutzung notwendig (Konto- und Anmeldedaten wie Name, Adresse, Telefonnummer, gegebenenfalls Zahlungsinformationen)?
- Welche Nutzungsbedingungen und Datenschutzerklärung schreibt der Anbieter vor? – (Hier ist speziell auf die Weitergabe von Inhalten zu achten.)
- Welche personenbezogenen oder sensiblen Daten möchte ich in einer Cloud anwenden/bearbeiten?
- Befindet sich der Cloud-Standort (Server) innerhalb der Europäischen Union (EU)? (dann greift die Datenschutzgrundverordnung, DSGVO) Kann das deutsche Datenschutzrecht angewendet werden?

- Wie viele Personen sollen den Dienst außerdem nutzen?
- Daraus abgeleitet: Wer soll gegebenenfalls spezielle Rechte bekommen?
- Ist eine regelmäßige Datensicherung beziehungsweise ein Backup außerhalb der Cloud (physische Speichermedien, z. B. mittels externer Festplatte) sinnvoll?
- Welche Sicherheitsmaßnahmen stehen zur Verfügung (Zwei-Faktor-Authentisierung, Datenverschlüsselung)?

Achtung:

Anbieter aus den USA, die einen Server-Standort in der EU haben, können momentan durch den „Cloud Act“ zur Herausgabe von Daten an US-Behörden verpflichtet werden – trotz geltender DSGVO.



Stellen Sie sicher, dass Sie bei bereits aktiven Anwendungen sichere Passwörter verwenden (weitere Hinweise hierzu finden Sie auch in Handreichung Nr. 2 „Surfen im Internet – zu Hause und mobil“) und dass sowohl das System als auch die einzelnen Dienste auf dem neuesten Stand sind (je nach Zugangsart immer die aktuellsten Updates zur jeweiligen App oder dem Web-Browser installieren). Äußerst empfehlenswert ist eine Zwei-Faktor-Authentifizierung (2FA):

Zusätzlich zu den Zugangsdaten muss ein weiterer Identitätsnachweis erbracht werden, beispielsweise durch die Eingabe eines Codes, der an das eigene Smartphone geschickt wurde.

Insbesondere bei Cloud-Speicher-Diensten wie *Google Drive* beziehungsweise *Google One*, *Amazon Drive*, *Microsoft Onedrive* oder *Dropbox* muss klar sein, dass von den Unternehmen Daten gesammelt werden – wenn auch in unterschiedlicher Intensität und aus verschiedenen Gründen. Oft hat man als Nutzer die Wahl zwischen eher lockeren Datenschutzbestimmungen, geringen Kosten und viel Speicherplatz auf der einen Seite oder einem DSGVO-konformen Umgang mit den hochgeladenen Inhalten zu höheren Kosten und mit geringerem Speicherumfang. Helfen können Verschlüsselungs-Tools wie *Boxcryptor*, die Dateien vor dem Hochladen in die Cloud codieren und so vor dem Zugriff durch Administratoren oder andere Stellen schützen. Bei der Ende-zu-Ende-Verschlüsselung ist das Decodieren nur mit Ihrem persönlichen Passwort möglich, was zu Einbußen im Nutzerkomfort führen kann.

Generell ist zu empfehlen, besonders sensible und private Daten nicht in einem Cloud-Speicher zu hinterlegen. Für Musik, Videos oder Bilder ist dieser eher geeignet.



Frage: Welche Art von Daten haben Sie bei welchen Anbietern gespeichert?

Datenlöschung und Wiederherstellung

Jede Datei hinterlässt Spuren in einem System. Selbst wenn sie in den Papierkorb verschoben und dieser geleert wird, ist das streng genommen noch kein Löschvorgang – diesen Umstand machen sich zum Beispiel IT-Forensiker zunutze. Im Grunde entfernt man damit nur die Pfade zur Datei, also die Information, wo diese zu finden ist. Zwar wird der Ort, an dem die Dateien liegen, zum Überschreiben freigegeben, doch erst wenn das geschehen ist, wird eine Datei tatsächlich gelöscht. Das übernehmen eigens dafür ausgerichtete Programme wie *Fileshredder* oder das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene *Darik's Boot and Nuke* (DBAN). Dieser Vorgang ist auf dem eigenen Rechner schnell umgesetzt. Problematisch kann es werden, wenn Sie Inhalte in einer Cloud abgelegt haben. Möchten Sie hier bewusst Dateien löschen, werden diese oft nicht sofort dauerhaft entfernt, sondern gelangen zunächst in eine Art virtuellen Papierkorb. Beim Anbieter *Dropbox* beispielsweise können Sie dort die Option „Endgültig löschen“ auswählen – ob, wann und wie das geschieht, darauf haben Sie bei keinem Anbieter direkten Einfluss. Sie müssen darauf vertrauen, dass der Vorgang in allen Datenbanken und Backup-Systemen vollzogen wird. Daher sollten Daten verschlüsselt werden, bevor Sie sie in die Cloud hochladen. Dafür gibt es diverse Tools wie *Boxcryptor* oder *Cryptomator*, die das übernehmen. Alternativ kann man bei bestimmten Dateiformaten wie PDF mit Passwortschutz arbeiten oder auf Cloud-Speicher wie *tresorit* setzen, die bereits eine integrierte Verschlüsselung anbieten.

Sollten Sie unabsichtlich Inhalte entfernt haben, wird das eben erläuterte Lösungsverfahren womöglich zu Ihrem Vorteil. Wie lange Sie gelöschte Dateien wiederherstellen können, variiert jedoch von Anbieter zu Anbieter. Unterschiede gibt es in der Regel außerdem je nach gewählter Nutzungsart: Wenn Sie die kostenlose Basis-Version eines Dienstes verwenden, ist die Speicherfrist für gelöschte oder überschriebene Daten für gewöhnlich kürzer als bei einem Geschäftskonto oder anderen kostenpflichtigen Tarifen. So werden bei *Dropbox* beispielsweise standardmäßig alle hinterlegten Datei-Versionen separat für 30 Tage gespeichert. In der „Professional“-Variante für Einzelpersonen ist eine Wiederherstellung innerhalb von 120 Tagen möglich.

Bei der *MagentaCLOUD* wird statt mit einzelnen Dateiversionsverläufen mit kompletten Sicherungen gearbeitet. Unter dem Punkt „Automatische Dateisicherung“ können Sie auswählen, in welchem zeitlichen Abstand Sicherungen all Ihrer Daten angelegt werden sollen: Täglich, wöchentlich oder monatlich. Die regelmäßig angelegten Sicherungen haben eine maximale Vorhaltezeit von sechs Monaten. In den Einstellungen können Sie diesen Wert aber auch auf eine Woche, einen Monat oder drei Monate setzen.

TIPP

Kürzere Vorhaltezeiten sind sinnvoll, wenn Sie Speicherplatz in Ihrer Cloud sparen wollen, da die Sicherungen auf diesen zugreifen. Richten Sie die Einstellungen nach Ihren Nutzungsgewohnheiten aus: Verwalten Sie beispielsweise auch berufliche Dateien in Ihrer Cloud und verwenden beziehungsweise bearbeiten diese mehrfach in der Woche, empfiehlt sich womöglich eine tägliche Sicherung mit eher kürzerer Bereithaltungsdauer. Nutzen Sie die Cloud vornehmlich als Datenspeicher für Foto-Ordner, die sie für gewöhnlich selten bearbeiten, würde sich eine monatliche Sicherung mit einer eher längeren Vorhaltezeit anbieten.

Ist die gewählte Bereithaltungsdauer abgelaufen, werden die Daten endgültig entfernt. Zusätzlich haben Sie die Möglichkeit manuelle Sicherungen anzulegen, die keiner festen Speicherfrist unterliegen, sondern dauerhaft abrufbar sind.

Wollen Sie die Sicherung vom 19. Jan. 2016 00:03 Uhr wiederherstellen? Die Dateien und Ordner aus der Sicherung werden in einen neuen Ordner kopiert. Der aktuelle Stand Ihrer MagentaCLOUD wird nicht überschrieben. Die Wiederherstellung wird im Hintergrund ausgeführt und kann einige Minuten dauern. Sie finden die wiederhergestellten Dateien in dem Ordner "Wiederhergestellte Dateien vom 19. Jan. 2016".

Wiederherstellung einer Sicherung in der MagentaCLOUD

Wenn Sie eine automatisch oder manuell erstellte Sicherung wiederherstellen wollen, werden sämtliche darin enthaltene Dateien in einen neuen Ordner kopiert, Ihre vorhandenen Cloud-Inhalte bleiben davon unberührt.

Freigabe-Optionen und Passwortschutz

In Cloudspeichern und Kollaborations-Anwendungen können Sie Inhalte für andere Nutzer freigeben. Überlegen Sie gut, ob andere Personen die Datei bearbeiten, kommentieren oder nur ansehen dürfen. Unter Umständen gibt es Einschränkungen durch den verwendeten Dienst (beispielsweise müssen benachrichtigte Personen bei *Google Drive* ein *Google*-Konto besitzen, andernfalls können sie trotz erteilter Berechtigung die Datei lediglich ansehen). Wichtig ist zudem der Status als „Eigentümer“ oder „Admin“ einer Datei: Nur dieser kann die Datei löschen und die Freigaben verwalten. Achten Sie darauf, ob Personen, die von Ihnen eine Freigabe zur Bearbeitung erhalten haben, wiederum selbst weitere Personen einladen können oder nicht. Unter Umständen können Sie auch ein Ablaufdatum festlegen, nach dem eingeladene Nutzer keinen Zugriff mehr bekommen, oder der Download von Inhalten verhindert wird. Die Freigabe-einstellungen lassen sich in der Regel jederzeit ändern und anpassen. Eine Einladung über E-Mail wird bei sensiblen Inhalten, die für einen kleinen Kreis bestimmt sind, empfohlen. Der Empfänger muss sich dabei mit seinem Konto in der Cloud anmelden.

Bei der Freigabe über Links ist dies nicht der Fall. Jeder, der den Link erhält, kann je nach eingestellter Berechtigung das Element anzeigen oder bearbeiten. Womöglich bekommen ihn auf diese Weise auch Personen, die Sie nicht persönlich kennen. Diese Option ist eher sinnvoll, wenn Sie schnell einen großen Kreis an Menschen erreichen wollen, in dem Sie beispielsweise eine Umfrage als Link über soziale Netzwerke teilen. Haben Sie Inhalte mit einem Passwort geschützt, sollten Sie es auf separatem Wege (bestenfalls per SMS oder Ähnlichem) zukommen lassen, ohne dass eine Zuordnung zum Zielinhalt möglich ist.

Rechtliche Datenschutzbestimmungen

Am 25. Mai 2018 ist die Datenschutzgrundverordnung (DS-GVO) in Kraft getreten. Sie definiert und schützt die Verarbeitung personenbezogener Daten innerhalb der EU. In Deutschland greift zusätzlich das Bundesdatenschutzgesetz. Datenschutzrechtlich fällt die Nutzung von Cloud-Diensten in den Bereich Auftragsverarbeitung. Im Auftrag des Nutzers werden Daten durch den Anbieter verarbeitet. Allerdings muss bei jedem Anbieter einzeln entschieden werden, welche Nutzung konkret vorliegt, woraus sich unterschiedliche Rechte und Pflichten ergeben (beispielsweise weisen Cloud-Speicher-Dienste schwerpunktmäßig einen Mietcharakter auf).

Ob die DSGVO oder ein anderes Datenschutzrecht für den Schutz der eigenen Daten herangezogen werden kann, ist rechtlich nicht immer eindeutig. Mitentscheidend ist der

Standort des Nutzers als auch der des Anbieters. Sobald personenbezogene Daten involviert sind und Nutzer als auch Anbieter ihren Standort in Deutschland haben, ist das deutsche Datenschutzrecht allerdings immer anwendbar. Schwieriger wird es bei Anbietern außerhalb der EU. Das EU-US-Datenschutzschild (Privacy Shield) soll zwar das Schutzniveau amerikanischer Dienstleister an europäische Maßstäbe annähern. Allerdings gilt seit März 2018 auch der „Cloud Act“: Das US-Gesetz erlaubt die Überwachung von Daten in der Cloud durch US-Behörden – selbst wenn sich diese im Ausland befinden. Ein US-Anbieter mit Server-Standort in Europa dürfte zwar Widerspruch dagegen einreichen, wenn die Betroffenen keine US-Bürger sind, vor Gericht käme es dann aber zu einer Interessensabwägung. Betroffene haben selbst keine Handhabe und müssen laut „Cloud Act“ nicht einmal über den Zugriff informiert werden. Doch nicht nur deshalb gelten außer-europäische Anbieter wie *Google*, *Microsoft* und *Amazon* als datenschutztechnisch bedenklich. Daher empfiehlt es sich ohnehin, immer die Nutzungsbedingungen der Dienstleister genau durchzulesen.

Cloud-Zertifizierung

Um beim Umgang mit Cloud-Diensten Rechtssicherheit zu haben, wurde in Deutschland 2010 die Initiative „Cloud Services Made in Germany“ gestartet. Anbieter, die der Initiative angehören, zeichnen sich unter anderem dadurch aus, dass sie in Deutschland gegründet wurden und dort ebenfalls ihren Hauptsitz haben, es einen lokal ansässigen deutsch-

sprachigen Service gibt und sie in allen juristischen Fragen dem deutschen Recht und Datenschutz unterliegen. Weitere Hinweise auf Informationssicherheit geben beispielsweise das IT-Grundschutz-Zertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie die Gütesiegel *SaaS* von *EuroCloud* und *TÜV Trust IT*.

Private Clouds als Alternative

Mit etwas technischem Know-how lassen sich private Clouds auch selbst anlegen. Damit umgeht man vielleicht unpassende Datenschutzbestimmungen großer Anbieter, ist allerdings allein für die Funktionalität verantwortlich. Beachten sollten Sie die nötigen Ressourcen, ob die Verwaltung über ein Webinterface möglich ist und welche Apps für welche Geräte angeboten werden (Smartphone, Tablets).

» Link-Tipp:

Eine kleine Anleitung dazu hat das Fachmagazin „PC-Welt“ veröffentlicht:
<https://kurzelinks.de/private-cloud-anlegen>

Glossar

Administrator: Rolle eines Benutzers in einem Betriebssystem, einer Anwendung oder auf einer Seite, die bestimmte erweiterte Rechte zur Veränderung oder Bearbeitung innehaben.

Automatische Sicherung: Speicherabbild eines Computersystems, das in einem festgelegten Intervall oder nach einer definierten Aktion selbstständig vom System erstellt wird.

Backup: Speicherabbild eines Computersystems (oder Teile davon) zu einem bestimmten Zeitpunkt, das für die Wiederherstellung desselbigen verwendet werden kann.

Bearbeitungsrechte: Befugnisse, die eine Nutzerin oder ein Nutzer in einem Computersystem haben. Bei Dateien kann das vom reinen Lesezugriff bis hin zu Schreib- und Vervielfältigungsrechten gehen.

Bundesdatenschutzgesetz: Das in Deutschland geltende Recht zum Umgang mit personenbezogenen Daten.

Client: Computerprogramm, das auf einem Endgerät ausgeführt wird und dabei mit einem Server (s.u.) kommuniziert.

Cloud-Speicher: Dateiverwaltung, bei der die Informationen nicht lokal auf dem Rechner gesichert werden, sondern

über Server auf einer virtuellen Festplatte liegen und daher jederzeit von überall abgerufen werden können.

CPU: Englisch central processing unit; der Zentralprozessor, der die Befehle eines Rechensystems verarbeitet

DSGVO: Die Datenschutz-Grundverordnung ist eine seit Mai 2018 geltende Verordnung in der Europäischen Union, die die Regeln zur Verarbeitung personenbezogener Daten länderübergreifend vereinheitlicht.

Freemail-Anbieter: E-Mail-Dienstleister, die für die Nutzung keine Gebühren erheben. Dafür sind diese oft werbelastig oder haben einen geringen Funktionsumfang.

Freigabeoptionen: Einstellmöglichkeit, wer in welchem Umfang Zugriff auf Dateien haben soll (siehe auch Bearbeitungsrechte).

Instant-Messaging-Dienste: Kommunikationsprogramme, bei denen die Nutzer in Echtzeit und unmittelbar (englisch instant) Textnachrichten und andere Inhalte austauschen können.

Manuelle Sicherung: Speicherabbild eines Computersystems, das vom Nutzer oder der Nutzerin per Befehl erstellt wird.

Passwortschutz: Definiert, ob, und falls ja, in welchem Maße der Zugriff auf eine Datei oder ein Nutzerkonto über ein zuvor festgelegtes Passwort gesichert ist.

RAM: Englisch random access memory; ein Datenspeicher, der in Computern als Arbeitsspeicher Verwendung findet und ein Merkmal der Leistungsfähigkeit eines Rechners darstellt.

Server: Beschreibt als Software ein Programm, das mit einem Client (s.o.) kommuniziert und diesem bestimmte Funktionen ermöglicht, so zum Beispiel den Zugriff auf eine Datenbank oder die Verwendung von Netzwerkdiensten.

Sicherung: Speicherabbild eines Computersystems

Synchronisierung: Abgleich und Aktualisierung der Daten auf verschiedenen Geräten beziehungsweise Speichermedien, um überall den gleichen Informationsstand zu erreichen.

Texteditoren: Computerprogramm zum Bearbeiten von Texten.

Verschlüsselung: Verfahren und Algorithmen, die Daten für Unbefugte mittels Codes oder Schlüssel in eine nicht mehr lesbare Form verwandeln.

Versionskonflikt: Synchronisierungsproblem, das auftritt, wenn eine Datei von verschiedenen Nutzern offline bearbeitet wurde und dann wieder zusammengeführt werden soll.

Vorhaltezeit: Zeitspanne, in der bereits gelöschte Daten noch auf dem Server verbleiben, bevor sie unwiderruflich entfernt werden.

Web-App/Web-Dienst: Eine Anwendung, die nicht im System installiert wird, sondern über den Browser gestartet und genutzt wird.

Webinterface: Grafische Benutzeroberfläche, die über den Browser beim Aufrufen einer Internetadresse angezeigt wird.

Wiederherstellung: Zurückversetzung eines Computersystems in einen bestimmten Zustand, der zuvor gespeichert wurde (siehe Backup und automatische/manuelle Sicherung).

Zertifikat: Gütesiegel, das einer Seite oder einer Anwendung bestimmte Eigenschaften attestiert.

Zwei-Faktor-Authentisierung: Identitätsnachweis eines Nutzers oder einer Nutzerin mit Hilfe zweier unterschiedlicher und voneinander unabhängigen Komponenten (beim Online-Banking beispielsweise Passwort und TAN).

Quiz

1. Sie möchten Inhalte Ihrer Cloud für andere freigeben. Welche Freigabe-Option ist sicherer?

- a) Ich teile die Inhalte über eine Einladung per Mail an die jeweiligen Personen.
- b) Ich generiere einen Link zu den Dateien und versende diesen.

2. Welche Aussage zu den Dateien in Ihrer Cloud stimmt?

- a) In meiner Cloud kann ich frei entscheiden, was ich hochlade. Dazu zählen auch fremde Inhalte wie Musik oder Videos.
- b) Ich kann frei entscheiden, was ich hochlade. Dennoch ist die Cloud kein rechtsfreier Raum. So sind beispielsweise die Nutzungsbedingungen des Cloud-Anbieters als auch das Urheberrecht zu beachten.

3. Ein Ordner in Ihrer Cloud wird nicht mehr benötigt und Sie entschließen sich dazu ihn zu löschen. Wie gehen Sie vor?

- a) Ich lösche den Ordner über den Web-Dienst oder den Client. Damit ist er nicht mehr auffindbar.
- b) Ich lösche den Ordner über den Web-Dienst oder den Client. Außerdem prüfe ich bei meinem Anbieter, ob der Ordner nur vorläufig entfernt wurde und bestätige gegebenenfalls den Vorgang mit dem Befehl „Endgültig löschen“. Dabei kann ich gleich die eingestellte Vorhaltezeit (siehe Glossar) überprüfen.

4. Sie arbeiten täglich mit vielen Dateien an Ihrem Rechner und in Ihrer Cloud. Vor allem viele Textdokumente werden oft bearbeitet. Welche Sicherungsvariante wählen Sie?

- a) Ich habe eine automatische Sicherung eingerichtet, die ein Mal pro Woche ein Backup erstellt. So bleibt der Datenverlust gering.
- b) Ich erstelle selbst unregelmäßig, meist nach Bauchgefühl, ein Backup.

Bestellung weiterer Handreichungen

Der Digital-Kompass wurde für Sie entwickelt: Sie erhalten die Möglichkeit, neues Wissen zu erwerben, Ihre gesammelten Erfahrungen auszutauschen und an ältere Menschen weiterzugeben. Hierfür bieten wir Ihnen didaktisch aufbereitete und für Sie kostenfreie Handreichungen, die Sie in Ihrem Engagement unterstützen sollen. Sie finden darin kompakte Informationen sowie praktische Übungsaufgaben, die Sie für den Austausch mit Ihren Seniorengruppen verwenden können.

- #1:** Was ist das Internet? Eine Einführung
- #2:** Surfen im Internet – Zu Hause und mobil
- #3:** Online-Kommunikation – E-Mails, Messenger und Videotelefonie
- #4:** Soziale Netzwerke im Internet – Miteinander in Kontakt bleiben
- #5:** Online-Einkaufen und Online-Banking – Sicher im Internet bestellen und bezahlen
- #6:** Reiseplanung im Internet
- #7:** Mediennutzung im Internet – Fotos, Musik und Videos
- #8:** Digitale Zukunft – Neue Anwendungen und Möglichkeiten
- #9:** Datenspeicherung im Internet

Bitte denken Sie daran, die Postadresse anzugeben, an die wir die Handreichungen schicken dürfen. Ihre personenbezogenen Daten werden wir ausschließlich im Rahmen dieses Bestellvorgangs verwenden. Wenn Sie fortlaufend über Neuigkeiten des Digital-Kompass informiert werden wollen, geben Sie das bitte bei Ihrer Bestellung zusammen mit Ihrer E-Mail-Adresse an – Sie erhalten dann einmal im Monat unseren Newsletter:

www.digital-kompass.de/newsletter

Digital-Kompass
c/o Deutschland sicher im Netz e.V.
Albrechtstraße 10 c, 10117 Berlin
Tel.: +49 (0) 30 27 57 63 77
Fax: +49 (0) 30 27 57 65 13 77
info@digital-kompass.de
www.digital-kompass.de



Eine Publikation von Deutschland sicher im Netz im Rahmen des Verbundprojekts **Digital-Kompass** mit der BAGSO – Bundesarbeitsgemeinschaft der Senioren-Organisationen und ermöglicht durch Förderung durch das Bundesministerium der Justiz und für Verbraucherschutz.

Der **Digital-Kompass** ist ein Treffpunkt für alle Fragen rund ums Internet und Co., die ältere Menschen bewegen. Auf www.digital-kompass.de gibt es vielfältige praxisnahe Materialien, Broschüren, Filme und Arbeitsblätter. Darüber hinaus finden Sie praktische Tipps für Treffen, Beratungen und Kurse rund um die digitale Welt.

Die Digitalen Stammtische ermöglichen einen Austausch zu aktuellen IT-Themen mit Experten und Gleichgesinnten deutschlandweit.

Bundesweit werden zahlreiche Digital-Kompass Standorte aufgebaut. Dort schaffen Internetlotsen eine vertrauensvolle (Lern-)Umgebung für ältere Menschen und unterstützen sie dabei, digitale Dienste auszuprobieren und einen souveränen Umgang mit dem Internet zu erlernen. Die Digital-Kompass Standorte sind zugleich Anlaufstellen für Internetlotsen, die sich weiterbilden oder in das Projekt einbringen möchten.



info@digital-kompass.de
www.digital-kompass.de



Gefördert durch:



Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

www.digital-kompass.de