

Zusammenfassung

Online-Zusammenarbeit



EASY4ME ✓

1. Konzepte der Online-Zusammenarbeit

Die Entstehung der digitalen Zusammenarbeit

Mit dem Aufkommen des Internets in den 1990er-Jahren entstanden völlig neue Möglichkeiten der Zusammenarbeit. Eine E-Mail erreicht den Empfänger weltweit innerhalb weniger Sekunden.

Die Sprachübertragung über das Internet (VoIP) veränderte die klassische Telefonie grundlegend, und Textnachrichten in Echtzeit (Chat) wurden schnell zum Standard der digitalen Kommunikation.

Moderne Technologien im Alltag

Die technologische Entwicklung hat sich stark beschleunigt. Heute gehören Videoübertragungen, Cloud-Speicher und die gemeinsame Bearbeitung von Dokumenten über das Internet zum Alltag.

Anwendungsbereiche von Online-Tools

Unternehmen mit internationalen Standorten sowie Schüler und Studierende nutzen digitale Werkzeuge für die Zusammenarbeit.

Die Online-Zusammenarbeit (OZ) wird sowohl im privaten Bereich (z. B. Schule, Studium, Vereine) als auch im beruflichen Umfeld eingesetzt. Häufig verwendete Tools sind beispielsweise:

- Google Workspace (Google Drive, Docs, Meet)
- Microsoft 365 (OneDrive, Word, Excel, Teams)

In Unternehmen steht dabei die Verbesserung von Arbeitsprozessen und Informationsflüssen im Vordergrund. Teams können weltweit ohne Zeitverlust zusammenarbeiten. Online-Meetings und Cloud-Arbeit ersetzen viele Dienstreisen, da ein gemeinsamer physischer Arbeitsplatz nicht mehr notwendig ist.

2. Cloud-Computing – „Rechnen in der Wolke“

Unter Cloud-Computing versteht man IT-Angebote wie Rechenleistung, Datenspeicher oder Software, die Anwendern flexibel über ein Netzwerk wie das Internet bereitgestellt werden.

Die Cloud kann man sich als entfernten Verbund aus Rechenzentren und Servern vorstellen, die dauerhaft online sind. Dort werden Daten zentral gespeichert und können von berechtigten Personen jederzeit abgerufen und bearbeitet werden. Änderungen sind sofort für alle sichtbar.

Vergleich zu früher: Früher mussten Dokumente umständlich per E-Mail zwischen den Anwendern hin und her geschickt werden. Dabei ging schnell die Übersicht verloren, welche Datei tatsächlich die aktuelle Version enthielt.

Beim Cloud-Computing werden Daten und Programme auf externe Rechenzentren eines Cloud-Anbieters (Cloud-Provider) ausgelagert. Die Anwendungen und Daten befinden sich nicht mehr auf der lokalen Festplatte des eigenen PCs oder im hauseigenen Firmenrechenzentrum, sondern oft geografisch weit entfernt. Der Zugriff erfolgt über das Internet, wodurch lokale Datenträger wie USB-Sticks oder externe Festplatten weniger wichtig werden.

Für den Anwender oder ein Unternehmen ergeben sich dadurch erhebliche Ersparnisse, da der eigene Aufwand für teure Hardware-Anschaffungen, Software-Wartung und lokale Backups sinkt.

2.1. Das Benutzerkonto (User Account)

Für die Nutzung von Cloud-Diensten ist ein Benutzerkonto erforderlich. Es dient als persönlicher Zugang zu einem System.

Beim Login erfolgt eine **Authentifizierung** mit Benutzername und Passwort. Dadurch erkennt das System den Nutzer und weist ihm bestimmte **Zugriffsechte** auf die vorhandenen Ressourcen (Programme, Speicherplatz, Ordner und Dateien) zu.

- **Beispiel Lagerverwaltung:** Herr Maier arbeitet im Lager. Über sein Benutzerkonto darf er die aktuellen Lagerbestände einsehen und verändern, er hat jedoch keinerlei Zugriff auf die vertraulichen Personalakten der Firma.
- **Beispiel Personalabteilung:** Frau Lainer arbeitet in der Lohnbuchhaltung. Ihr Benutzerkonto gewährt ihr Zugriff auf alle Mitarbeiterdaten, die für die Berechnung des Lohnes und der Abgaben zwingend erforderlich sind.

2.2. Vorteile von Cloud-Computing

- **Kostenersparnis:** Die Datenverarbeitung erfolgt in externen Rechenzentren des Anbieters. Dadurch entfallen hohe Investitionen für eigene Server-Hardware, Klimatisierung der Serverräume und das dafür notwendige IT-Fachpersonal.
- **Skalierbarkeit:** Wird kurzfristig mehr Speicherplatz oder eine höhere Rechenleistung benötigt, kann diese beim Cloud-Anbieter mit wenigen Klicks bestellt werden und steht sofort bereit. Es muss keine neue Hardware gekauft werden.
- **Erhöhte Zuverlässigkeit (Ausfallsicherheit):** Große Cloud-Anbieter betreiben mehrere, geografisch getrennte Rechenzentren. Sollte ein Rechenzentrum ausfallen, übernehmen gespiegelte Systeme sofort und automatisch die Arbeit. Der Anwender merkt von dieser Störung in der Regel nichts.
- **Hohe physische Sicherheit:** Die professionellen Rechenzentren der Cloud-Provider sind durch modernste Sicherheitssoftware, Zugangskontrollen und Brandschutzsysteme geschützt, die ein normales Unternehmen kaum finanzieren könnte.
- **Erhöhte Mobilität:** Daten und Dienste sind plattformunabhängig und überall verfügbar. Mitarbeiter können im Homeoffice, im Zug oder beim Kunden via Tablet, Notebook oder Smartphone exakt so arbeiten wie im Büro. Voraussetzung ist lediglich eine aktive Internetverbindung.
- **Web-basierte Office-Anwendungen:** Programme müssen nicht mehr zwingend lokal auf dem PC installiert sein. Werkzeuge wie Google Docs oder Microsoft 365 laufen direkt im Webbrowser und werden vom Anbieter oft in einer kostenlosen Basisversion bereitgestellt.

- **Gleichzeitiger Zugriff (Dokument-Sharing):** Mehrere Personen können zeitgleich an ein und demselben Dokument arbeiten. Da nur noch eine einzige Version in der Cloud existiert, gehören doppelte Datenbestände der Vergangenheit an. Die Bearbeitung ist auch problemlos auf mobilen Geräten möglich.
- **Einfache Freigabe:** Dokumente werden zeitsparend freigegeben, indem man eine Einladung per E-Mail versendet oder einen direkten Freigabelink generiert.
- **Globale Reichweite:** Der Zugriff auf alle benötigten Dokumente, Termine und Programme kann von jedem Ort der Welt aus erfolgen.

2.3. Risiken von Cloud-Computing

- **Datenschutz und Datensicherheit:** Da sensible Daten das eigene Gerät und das firmeninterne Netzwerk verlassen, steigt das Risiko für unberechtigte Zugriffe von außen (Cyber-Spionage, Hackerangriffe). Es muss genau geprüft werden, in welchem Land die Server physisch stehen und ob die dortigen Gesetze den strengen Vorgaben der europäischen **DSGVO** entsprechen.
- **Abhängigkeit von Verbindung und Anbieter:** Wenn die eigene Internetverbindung ausfällt oder der Cloud-Anbieter eine serverseitige technische Störung hat, ist kein Zugriff auf die Daten möglich. In diesem Moment steht der gesamte Arbeitsbetrieb still.

2.4. Technische Voraussetzungen für eine funktionierende OZ

- **Sichere Netzwerkverbindung:** Die Datenübertragung im Internet muss verschlüsselt erfolgen. Im Webbrowser ist dies leicht am Protokoll **https** (das „s“ steht für secure) sowie am geschlossenen Schloss-Symbol in der Adresszeile zu erkennen.
- **Schnelle Netzwerkverbindung:** Die verfügbare Bandbreite ist ein kritischer Faktor. Sowohl die **Download-** als auch die **Upload Geschwindigkeit** müssen ausreichend hoch sein, um flüssiges Arbeiten im Cloud-Speicher und eine ruckelfreie Bild- und Tonübertragung bei Videokonferenzen zu garantieren.
- **Beständige Netzwerkverbindung:** Die Verbindung muss stabil und ohne permanente Abbrüche zur Verfügung stehen, da die Online-Tools sonst die Synchronisation verlieren.

3. Wichtige Tools zur Online-Zusammenarbeit

3.1. Office-Anwendungen und Produktivitätssysteme

- **Microsoft 365:** Vereint den Online-Speicher OneDrive mit web-basierten Versionen der klassischen Office-Programme (Word, Excel, PowerPoint, OneNote) und Kommunikationstools (Outlook für E-Mail und Kalender, Microsoft Teams).
- **Google Workspace:** Stellt über den Online-Speicher Google Drive Anwendungen für Textverarbeitung (Docs), Tabellenkalkulation (Sheets) und Präsentationen (Slides) zur Verfügung.

3.2. Cloud-Speicher (Online-Datenspeicher)

Bekannte Plattformen sind OneDrive, Google Drive und Dropbox. Daten werden nicht mehr nur lokal auf dem Computer gesichert, sondern direkt in den Cloud-Speicher hochgeladen. Dies schont den physischen Speicherplatz auf Mobilgeräten (Smartphones, Tablets), da die Dateien direkt online abgerufen und verarbeitet werden.

- **Berechtigungsstufen (Rechtevergabe):** Bei der Freigabe einer Datei kann exakt definiert werden, welche Rechte der Empfänger besitzt. Man unterscheidet primär zwischen **Leserechten** (nur ansehen) und **Schreibrechten** (ansehen und bearbeiten).
- **Versionsverwaltung:** Das System speichert bei jeder Änderung automatisch den alten Zustand der Datei in einem Archiv ab, verknüpft mit der mit Informationen zum Bearbeiter und Zeitpunkt. So lässt sich nachvollziehen, wer welche Änderungen durchgeführt hat, und ältere Stände können bei Fehlern sofort wiederhergestellt werden.
- **Versionskonflikt:** Wenn zwei Personen gleichzeitig offline an getrennten Kopien derselben Datei arbeiten und diese anschließend hochladen, kann das System die Daten nicht automatisch zusammenführen. Um Datenverlust zu vermeiden, erstellt der Cloud-Speicher automatisch eine separate Dateikopie (z. B. Bericht-Kopie.docx).

3.3. Webkonferenz – Online-Meeting

Unter einer Webkonferenz versteht man ein virtuelles Treffen von Teilnehmern über das Internet, die sich an völlig unterschiedlichen Orten befinden können. Der Konferenzraum wird durch den Bildschirm des Moderators ersetzt.

- **Desktop-Sharing:** Der Moderator überträgt seinen Bildschirminhalt in Echtzeit auf die Monitore der Teilnehmer, um Präsentationen oder Software live vorzuführen.
- **Kommunikationskanäle:** Die Interaktion erfolgt primär per Sprache und Video (Webcam). Parallel dazu verfügt jedes moderne Konferenztool über einen integrierten **Chat**, über den die Teilnehmer Textbeiträge, Fragen oder Links austauschen können, ohne den Redner zu unterbrechen.
- **Tools:** Gängige Anwendungen sind Microsoft Teams oder Google Meet. (Hinweis: Der ehemals populäre Dienst Skype wurde in diesem Bereich weitgehend durch Teams abgelöst).

3.4. Soziale Medien (Social Media)

Soziale Medien ermöglichen es Nutzern, digitale Inhalte zu veröffentlichen, Kontakte zu pflegen und sich auszutauschen.

- **Soziale Netzwerke:** Plattformen wie Facebook, Instagram oder WhatsApp dienen der schnellen, meist privaten Kommunikation.
- **Mikroblogging:** Plattformen zur Veröffentlichung kurzer Textnachrichten oder Postings. Die Beiträge sind meist öffentlich und werden in chronologisch umgekehrter Reihenfolge dargestellt (neue Nachrichten stehen ganz oben). Der bekannteste Dienst ist **X** (ehemals Twitter).

- **Newsgruppen und Foren:** Webseiten, auf denen Beiträge zu spezifischen Fachthemen zeitversetzt diskutiert werden. Zur aktiven Teilnahme ist in der Regel das Erstellen eines Benutzerkontos erforderlich.
- **Wikis:** Wissensplattformen, deren Inhalte von den Anwendern nicht nur gelesen, sondern direkt online über den Webbrowser editiert und erweitert werden können. Das bekannteste Beispiel ist Wikipedia.
- **Multimedia-Sharing:** Portale zum Hochladen und Teilen von Fotos und Videos (z. B. YouTube, Flickr).
- **Einsatz im Beruf:** Im geschäftlichen Umfeld ist die Nutzung privater Social-Media-Tools auf Firmenrechnern meist untersagt. Das Risiko, dass vertrauliche Unternehmensdaten an die Öffentlichkeit gelangen oder Schadsoftware eingeschleust wird, ist zu hoch. Stattdessen nutzen Firmen geschlossene, interne Plattformen.
- **Digitaler Fußabdruck:** Einmal im Internet veröffentlichte Inhalte (Fotos, Kommentare) lassen sich nur sehr schwer oder teilweise überhaupt nicht mehr vollständig löschen.

3.5. Online-Kalender und Terminverwaltungen

Digitale Kalender optimieren die Zeitplanung innerhalb von Teams und Organisationen:

- **Freigaben:** Kalender können für Kollegen freigegeben werden. Zur besseren Übersicht lassen sich die Kalender der Teammitglieder flexibel ein- und ausblenden.
- **Einladungsmanagement:** Bei der Erstellung eines Termins werden Einladungen automatisch per E-Mail an die Teilnehmer versandt. Die Empfänger können direkt im System zu- oder absagen, woraufhin der Status im Kalender des Organisators aktualisiert wird.
- **Suchfunktion:** Der gesamte Kalender ist über Suchbegriffe blitzschnell durchsuchbar.
- **Automatische Synchronisation:** Trägt man einen Termin am Smartphone ein, gleicht sich der Kalender über das Internet automatisch mit dem PC und dem Tablet ab. Alle Geräte sind permanent auf demselben Stand.
- **Erinnerungen:** Das System erinnert rechtzeitig per Pop-up-Meldung, E-Mail oder SMS an bevorstehende Termine.

3.6. Learning Management System (LMS) / Virtuelle Lernumgebung (VLE)

Ein LMS (wie Microsoft Teams oder Google Classroom) ist ein umfassendes Softwaresystem, das der Bereitstellung von Lerninhalten und der digitalen Organisation von Lehrgängen dient.

- **Lehrende** können Lernmaterialien (Texte, Videos, Skripte) hochladen, verwalten und den Kursen zuteilen.
- **Lernende** rufen die Aufgaben online ab, bearbeiten diese lokal oder direkt im Browser und laden die fertigen Ergebnisse zur Korrektur hoch.
- **Lernzielkontrollen:** Über integrierte, digitale Tests (**Quizze**) kann der Lernerfolg automatisch überprüft und ausgewertet werden.

- **Kommunikation:** Für Fragen und den Austausch untereinander stehen Diskussionsforen und integrierte Chats zur Verfügung.

4. Mobile Zusammenarbeit und Datenübertragung

Tragbare Elektronikgeräte wie Smartphones und Tablets ermöglichen das Arbeiten von jedem beliebigen Ort aus. Sie sind mit speziellen, mobilen Betriebssystemen ausgestattet:

- **Android:** Ein von Google entwickeltes, auf Linux basierendes Betriebssystem.
- **iOS:** Das proprietäre Betriebssystem¹ von Apple für das iPhone und das iPad.

Die Installation von Anwendungssoftware (Apps) erfolgt sicher über die zentralen Plattformen der Hersteller, den Google Play Store beziehungsweise den Apple App Store.

4.1. Übertragungstechnologien

Bluetooth² für Kurzstrecken

Bluetooth ist eine weltweit einheitliche Technologie für den kabellosen Datenaustausch über kurze Distanzen (Reichweite bis ca. 10 Meter) und zeichnet sich durch einen sehr geringen Energieverbrauch aus. Es wird vor allem genutzt, um Peripheriegeräte (Kopfhörer, Freisprechanlagen im Auto, Drucker oder Tastaturen) drahtlos mit dem Mobilgerät zu verbinden.

Sicherheitshinweis: Eine dauerhaft aktivierte Bluetooth-Funktion kann ein Risiko darstellen, da Angreifer bekannte Bluetooth-Sicherheitslücken ausnutzen können, um Daten auszulesen. Bluetooth sollte daher bei Nichtgebrauch immer deaktiviert werden.

Kabellose Verbindungen (WLAN / Wi-Fi)

- **WLAN (Wi-Fi):** Steht für *Wireless Local Area Network* (drahtloses lokales Netzwerk). Es verbindet Geräte ohne Kabel mit einem Router und ermöglicht so den Zugang zum Internet.
- **Öffentliche Hotspots:** Kostenlose WLAN-Zugangspunkte an öffentlichen Plätzen (z. B. Cafés, Hotels, Flughäfen). Da sie meist unverschlüsselt und für jeden frei zugänglich sind, gelten sie als unsicher. Unbefugte können den Datenverkehr in solchen Netzen leicht abfangen.

Schutzmaßnahmen in öffentlichen Netzwerken

Sensible Daten (wie Passwörter oder Online-Banking) dürfen in öffentlichen Netzwerken nur verschlüsselt übertragen werden. Dafür gibt es zwei zentrale Schutzmechanismen:

¹ Ein herstellereigenes, geschlossenes Betriebssystem (z. B. Apple iOS), dessen Quellcode geheim ist und ausschließlich vom Eigentümer verändert oder weiterentwickelt werden darf.

² Der Name leitet sich vom dänischen König Harald Blauzahn (Harald Blåtand) ab, der im 10. Jahrhundert Teile Dänemarks und Norwegens vereinte. Analog dazu soll die Bluetooth-Technologie unterschiedliche elektronische Geräte und Kommunikationsstandards drahtlos miteinander verbinden.

- **Das Protokoll HTTPS:** Verschlüsselt die Daten direkt zwischen dem Browser und der Webseite. Es ist erkennbar am Schloss-Symbol in der Adresszeile und ist immer beim Surfen sowie bei der Nutzung von Cloud-Tools absolut notwendig.
- **Das VPN (Virtual Private Network):** Sichert den gesamten Datenverkehr des Geräts über einen geschützten Datentunnel ab. Dies ist speziell beim Arbeiten in öffentlichen, unverschlüsselten Netzwerken notwendig (wichtig z. B. für Mitarbeiter im Außendienst), um Angriffe im selben WLAN zu verhindern.

5. Mobiles Internet

Mobiles Internet bezeichnet den weltweiten Datenzugriff von unterwegs über das Mobilfunknetz mittels Smartphones, Tablets oder Notebooks. Die Verbindung läuft dabei nicht über ein lokales WLAN, sondern über die Sendemasten der Mobilfunkanbieter.

Je nach Ausbau des Netzes vor Ort (z. B. mit den Standards **4G/LTE** oder **5G**) werden sehr hohe Übertragungsgeschwindigkeiten erreicht. Das mobile Netz ist heute so gut ausgebaut, dass Daten, Videos und Webseiten fast überall ohne Verzögerung geladen werden können.

Mobiler Internetzugang (Tethering)

Mobiler Hotspot: Ein Smartphone kann so eingerichtet werden, dass es seine eigene Internetverbindung drahtlos mit anderen Geräten (wie einem Notebook oder Tablet) teilt. So kann man auch dort im Internet arbeiten, wo kein lokales WLAN vorhanden ist.

5.1. Auswahlkriterien für den passenden Anbieter

- **Netzabdeckung:** Das wichtigste Kriterium. Gibt an, ob und in welcher Signalqualität das mobile Internet an den Standorten, an denen man sich am häufigsten aufhält (Wohnort, Arbeitsplatz, Pendelstrecke), verfügbar ist.
- **Geschwindigkeit:** Die maximale Download- und Uploadrate des Tarifs.
- **Datenvolumen:** Das monatlich inkludierte Datenbudget (z. B. 20 GB) oder ein unbegrenzter Tarif (Flatrate). Bei Tarifen mit begrenztem Volumen wird nach dem Verbrauch des Budgets entweder die Geschwindigkeit drastisch gedrosselt oder es entstehen automatische Zusatzkosten.
- **Monatliche Fixkosten:** Die Grundgebühr des Mobilfunkvertrags.

5.2. Die Kostenfalle „Datenroaming“

Befindet man sich außerhalb des Heimatnetzes im Ausland, bucht sich das Gerät in ein fremdes Mobilfunknetz ein. Diesen Vorgang nennt man **Datenroaming**. Innerhalb der EU ist das Roaming durch gesetzliche Vorgaben meist kostenlos im Heimattarif inkludiert.

Sobald man jedoch in ein **Nicht-EU-Ausland** reist (oder sich auf Schiffen, Fähren und in Flugzeugen befindet, die eigene Satelliten-Netze nutzen), können pro übertragene Megabyte extrem hohe Kosten entstehen.

Um alle Gebühren mit **einem einzigen Klick** sicher zu verhindern:

1. **Den Flugmodus (Flugprofil) aktivieren:** Dies schaltet sofort das gesamte Mobilfunknetz und alle mobilen Daten ab.
2. **WLAN manuell wieder einschalten:** Im Flugmodus kannst du das WLAN separat wieder aktivieren, um dich mit kostenlosen, vertrauenswürdigen Netzen vor Ort zu verbinden.

6. Sicherheit und rechtliche Aspekte bei der Online-Zusammenarbeit

6.1. Absicherung mobiler Endgeräte

Da Smartphones und Tablets im mobilen Alltag leicht verloren gehen, im Zug liegen gelassen oder gestohlen werden können, ist eine konsequente Absicherung der Geräte Pflicht, um Folgeschäden durch Datendiebstahl zu verhindern:

- **Bildschirmsperre (PIN / Passwort / Biometrie):** Das Gerät muss durch eine PIN, ein starkes Passwort oder biometrische Merkmale (Fingerabdruck, Gesichtserkennung) vor unbefugtem Zugriff geschützt sein. Dies verhindert, dass Diebe Zugriff auf private Nachrichten, gespeicherte Passwörter oder hochsensible Apps (z. B. Banking-Apps oder Bezahl Dienste) erhalten.
- **Datenverschlüsselung:** Bei modernen Mobilgeräten ist der interne Speicher standardmäßig automatisch verschlüsselt. Dieser Schutz ist jedoch **nur dann wirksam**, wenn eine Bildschirmsperre (z. B. **PIN, Passwort oder biometrische Authentifizierung mittels Fingerabdrucks oder Gesichtserkennung**) eingerichtet ist. Ohne die korrekte Authentifizierung können die auf dem Speicherchip abgelegten Daten selbst bei physischem Zugriff auf das Gerät in der Regel nicht entschlüsselt werden.
- **Regelmäßige Backups (Sicherheitskopien):** Um sich vor dauerhaftem Datenverlust infolge eines Gerätedefekts, Verlusts oder Diebstahls zu schützen, sollten regelmäßig Backups erstellt werden. Diese Sicherungskopien können automatisiert in einem sicheren Cloud-Speicher oder manuell auf einem lokalen externen Speichermedium gespeichert werden. Im Schadensfall lassen sich Daten und Einstellungen dadurch schnell auf ein neues Gerät übertragen und wiederherstellen.

6.2. Schutz vor Gefahren aus dem Internet

- **Phishing:** Eine der größten Gefahren bei der Online-Zusammenarbeit. Angreifer versenden gefälschte E-Mails, Chat-Nachrichten oder SMS (oft perfekt als vermeintliche Cloud-Freigaben von OneDrive oder Google Drive getarnt). Das Ziel ist es, den Anwender auf manipulierte Webseiten zu locken, um dort seine persönlichen Anmeldedaten (Benutzername und Passwort) abzufangen.
- **Zwei-Faktor-Authentifizierung (2FA):** Diese Sicherheitsmaßnahme schützt Benutzerkonten effektiv. Neben der Eingabe des normalen Passworts (1. Faktor) wird ein zweiter, dynamischer Faktor benötigt (z. B. ein einmaliger Zahlencode per SMS oder eine Bestätigung über eine Authenticator-App auf dem Smartphone).

Selbst wenn ein Angreifer das Passwort durch Phishing erlangt, kann er sich ohne den zweiten Faktor in der Regel nicht anmelden.

- **Schadsoftware (Malware) und Firewalls:** Viren, Trojaner oder Spyware können über infizierte Dateianhänge, manipulierte Cloud-Freigaben oder den Download unseriöser Anwendungen auf ein Gerät gelangen. Eine Firewall überwacht und filtert als Schutzbarriere den ein- und ausgehenden Netzwerkverkehr eines Systems. Sie kann jedoch nicht verhindern, dass ein Anwender eigenständig eine infizierte Datei herunterlädt und ausführt. Eine Firewall ist daher in der Regel nur eine Ergänzung zu einem Antivirenprogramm.

6.3. Urheberrecht und geistiges Eigentum

- **Geistiges Eigentum (Intellectual Property):** Digitale Inhalte im Internet (z. B. Texte, Grafiken, Fotos, Videos oder Musikstücke) sind in der Regel urheberrechtlich geschützt, sofern sie eine ausreichende Schöpfungshöhe aufweisen und nicht gemeinfrei sind. Die Rechte an diesen Werken liegen beim jeweiligen Urheber bzw. Rechteinhaber.
- **Nutzungsrechte und Lizenzen:** Die bloße Verfügbarkeit eines Inhalts im Internet bedeutet nicht, dass dieser frei genutzt werden darf. Die Nutzung urheberrechtlich geschützter Werke ist nur im Rahmen gesetzlicher Schranken (z. B. für den privaten Gebrauch) oder aufgrund einer ausdrücklichen Erlaubnis bzw. Lizenz zulässig. Jede darüberhinausgehende Nutzung, etwa Veröffentlichung, Bearbeitung oder kommerzielle Verwendung, erfordert die Zustimmung des Rechteinhabers.

Inhaltsverzeichnis

1.	Konzepte der Online-Zusammenarbeit	2
2.	Cloud-Computing – „Rechnen in der Wolke“	2
2.1.	Das Benutzerkonto (User Account).....	3
2.2.	Vorteile von Cloud-Computing	3
2.3.	Risiken von Cloud-Computing	4
2.4.	Technische Voraussetzungen für eine funktionierende OZ.....	4
3.	Wichtige Tools zur Online-Zusammenarbeit	4
3.1.	Office-Anwendungen und Produktivitätssysteme.....	4
3.2.	Cloud-Speicher (Online-Datenspeicher)	5
3.3.	Webkonferenz – Online-Meeting	5
3.4.	Soziale Medien (Social Media)	5
3.5.	Online-Kalender und Terminverwaltungen	6
3.6.	Learning Management System (LMS) / Virtuelle Lernumgebung (VLE)	6
4.	Mobile Zusammenarbeit und Datenübertragung	7
4.1.	Übertragungstechnologien	7
5.	Mobiles Internet	8
5.1.	Auswahlkriterien für den passenden Anbieter	8
5.2.	Die Kostenfalle „Datenroaming“	8
6.	Sicherheit und rechtliche Aspekte bei der Online-Zusammenarbeit	9
6.1.	Absicherung mobiler Endgeräte	9
6.2.	Schutz vor Gefahren aus dem Internet	9
6.3.	Urheberrecht und geistiges Eigentum	10