

**1. Handlungsschritt (25 Punkte)**

Sie bereiten sich auf ein Gespräch mit der Media AG zum Thema Cloud-Computing vor.

a) Nennen Sie drei Vorteile von Cloud-Computing gegenüber einem eigenen Rechenzentrum. (3 Punkte)

* Einsparung von teilweise erheblichen Investitionen für Dienste, die in der Cloud einfach nur angemietet werden.
* Keine längerfristige Kapitalbindung, da die benötigten Dienste und Hardware angemietet werden, wofür klar kalkulierbare Kosten monatlich fällig werden.
* Skalierbarkeit der Dienste, d. h. je nach Nutzungsgrad können Ressourcen bedarfsweise angemietet werden, um z. B. Nutzungsspitzen auszugleichen oder schnell auf Wachstum zu reagieren.
* Mittels eines klar zu definierenden SLA erfolgt ein Risikotransfer vom eigenen Unternehmen in Richtung des Anbieters.
* Da Cloud-Anbieter ihre Ressourcen für viele Marktteilnehmer bereitstellen, können die einzelnen Dienstleistungen kostengünstiger angeboten werden, als dies ein Einzelunternehmen kann, das hierfür Personal, Hardware und Software bereitstellen muss.
* Man nutzt Ressourcen, die i. d. R. dem aktuellen Stand der Technik entsprechen bzw. laufend auf dem aktuellen Stand gebracht werden.
* Verschiedene regionale Standorte können kostengünstig an die Unternehmensressourcen angebunden werden.
* Verminderung der Abhängigkeit von den eigenen IT-Mitarbeitern.
* Höhere Ausfallsicherheit der Hardware in der Cloud durch leistungsfähigere USV, Redundanz, Zutrittsschutz etc.
* Hohe Kompetenz im Bereich IT durch den Cloud-Anbieter, die mit eigenen Personal nicht oder nur schwer realisiert werden könnte.

b) Cloud-Computing wird im Rahmen von drei Service-Modellen angeboten:

- Infrastructure as a service (IaaS)  
- Platform as a service (PaaS)  
- Software as a service (SaaS)

ba) Ordnen Sie die folgenden Dienste dem entsprechenden Service-Modell in nachstehender Tabelle zu. (6 Punkte)

- Betriebssystem  
- Datenbank  
- Entwicklungsumgebung  
- Netzwerk  
- Speicher  
- Software on demand

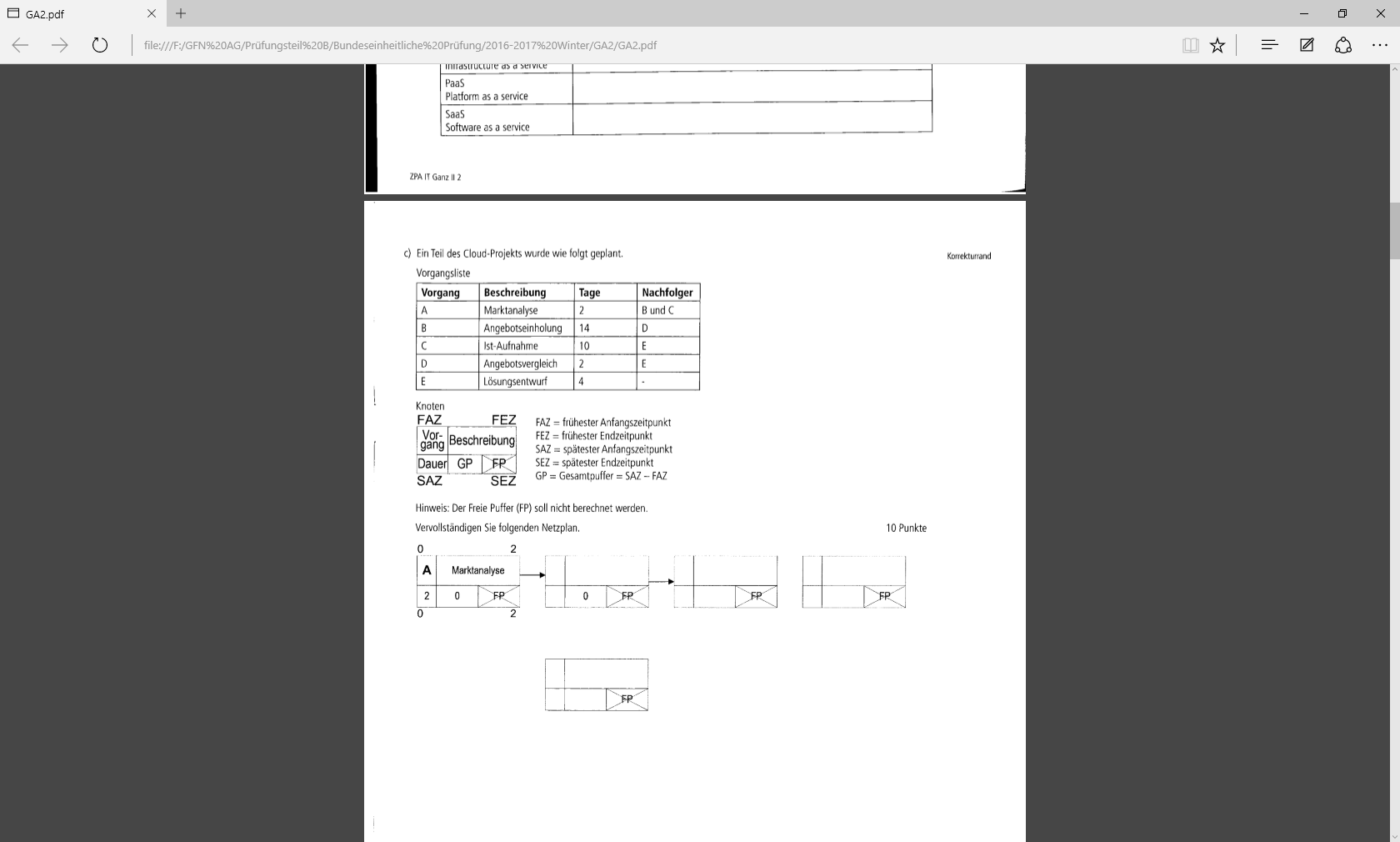
|  |  |
| --- | --- |
| **Service-Modell** | **Dienste des Service-Modells** |
| IaaS Infrastructure as a service | Speicher  Netzwerk |
| PaaS Platform as a service | Entwicklungsumgebung  Datenbank |
| SaaS Software as a service | Betriebssystem  Software on demand |

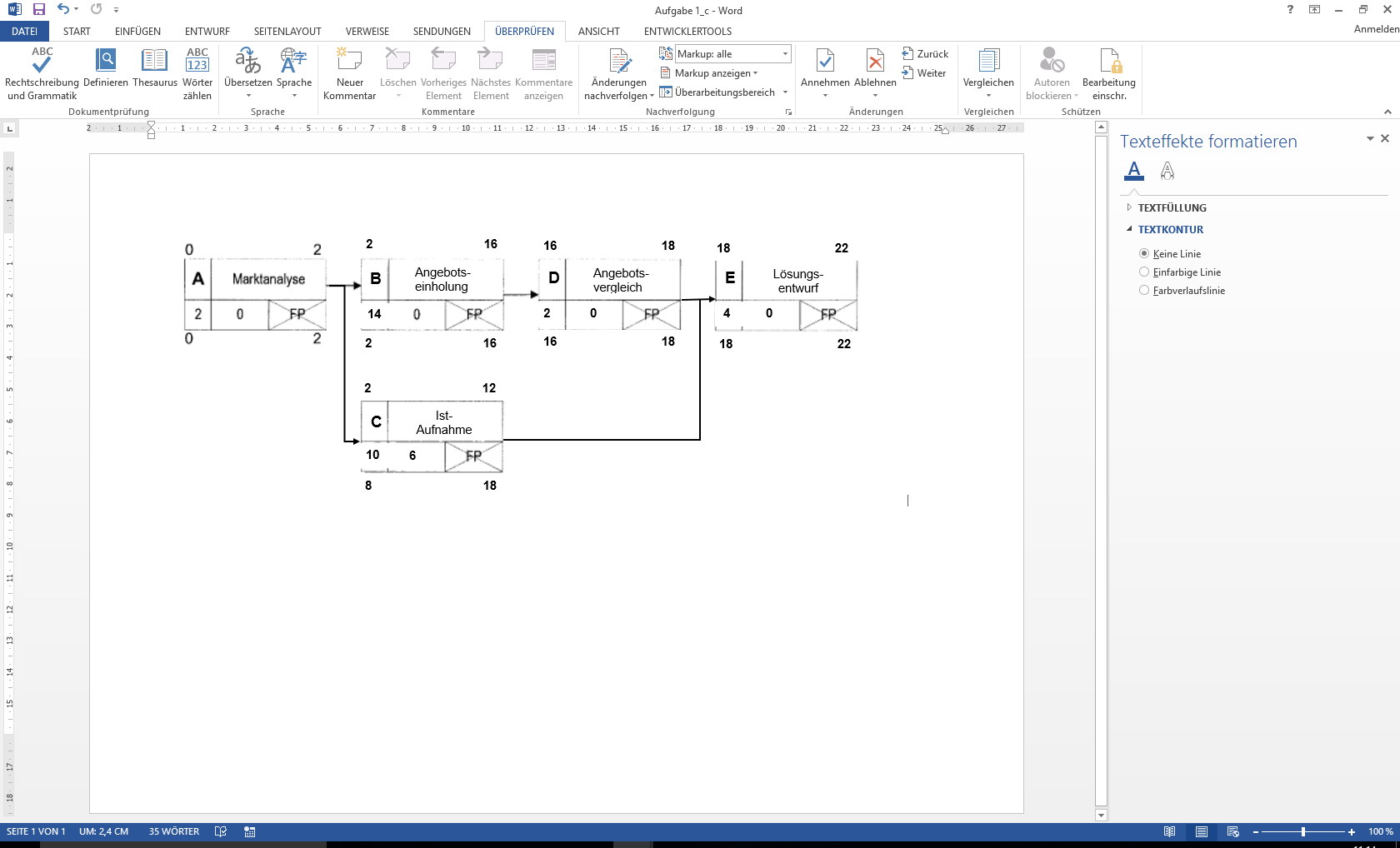
bb) Ordnen Sie die folgenden Anwendungen den entsprechenden Service-Modellen in nachstehender Tabelle zu. (6 Punkte)

- Onlinespiele  
- E-Mail-Systeme  
- VoIP-Telefonanlage  
- Web-Hosting mit Datenbank und Entwicklungssystem  
- Online Office-Anwendungen  
- Cloud Backup-System

|  |  |
| --- | --- |
| **Service-Modell** | **Anwendungsbeispiel** |
| IaaS Infrastructure as a service | VoIP-Telefonanlage  Cloud Backup-System |
| PaaS Platform as a service | Web-Hosting mit Datenbank und Entwicklungssystem |
| SaaS Software as a service | Onlinespiele  E-Mail-Systeme  Online Office-Anwendungen |

c) Ein Teil des Cloud-Projekts wurde wie folgt geplant:





**2. Handlungsschritt (25 Punkte)**

Die KLÜBERO GmbH soll die Media AG zu Cloud-Computing beraten.

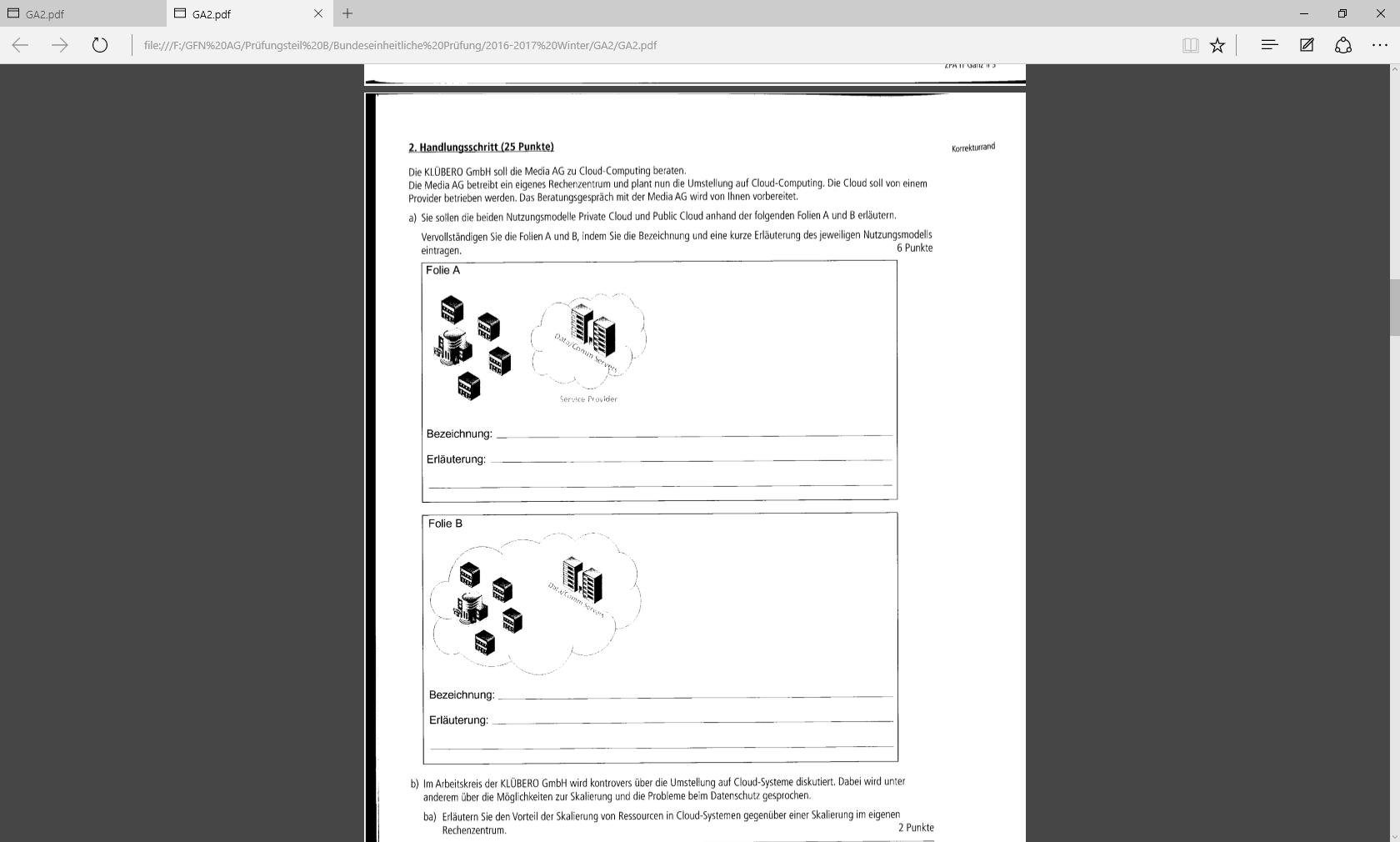
Die Media AG betreibt ein eigenes Rechenzentrum und plant nun die Umstellung auf Cloud-Computing. Die Cloud soll von einem Provider betrieben werden. Das Beratungsgespräch mit der Media AG wird von Ihnen vorbereitet.

a) Sie sollen die beiden Nutzungsmodelle Private Cloud und Public Cloud anhand der folgenden Folien A und B erläutern. Vervollständigen Sie die Folien A und B, indem Sie die Bezeichnung und eine kurze Erläuterung des jeweiligen Nutzungsmodells eintragen. (6 Punkte)



Folie A: Public Cloud

Die Public Cloud oder öffentliche Cloud ist ein Angebot eines frei zugänglichen Providers, der seine Dienste offen über das Internet für jedermann zugänglich macht. Webmailer-Dienste oder die bekannten Google-Docs sind ebenso Beispiele für Public Cloud Angebote wie die kostenpflichtigen Services eines Microsoft Office 365 oder eines SAP Business by Design.



Folie B: Private Cloud

Aus Gründen von Datenschutz und IT-Sicherheit ziehen es Unternehmen häufig vor, ihre IT-Dienste weiterhin selbst zu betreiben und ausschließlich ihren eigenen Mitarbeitern zugänglich zu machen.

Werden diese in einer Weise angeboten, dass der Endnutzer im Unternehmen cloud-typische Mehrwerte nutzen kann, wie z. B. eine skalierbare IT-Infrastruktur oder installations- und wartungsfreie  
IT-Anwendungen, die über den Webbrowser in Anspruch genommen werden können, dann spricht man von einer Private Cloud.

Cloud-Angebote stehen nur einem bestimmten Nutzerkreis, wie Angehörigen der gleichen Firma, offen, im Gegensatz zu Public-Cloud-Lösungen, die alle Interessierten verwenden können.

b) Im Arbeitskreis der KLÜBERO GmbH wird kontrovers über die Umstellung auf Cloud-Systeme diskutiert. Dabei wird unter anderem über die Möglichkeiten zur Skalierung und die Probleme beim Datenschutz gesprochen.

ba) Erläutern Sie den Vorteil der Skalierung von Ressourcen in Cloud-Systemen gegenüber einer Skalierung im eigenen Rechenzentrum. (2 Punkten)

Cloud-Diensteanbieter erlauben ihren Kunden, IT-Infrastruktur auf einer flexiblen Basis des Bezahlens für den tatsächlichen Nutzungsgrad bzw. Verbrauch (pay-as-you-go) zu mieten, ohne Kapital in Rechner- und Datenzentrumsinfrastruktur investieren zu müssen. Die notwendigen Ressourcen lassen sich so problemlos und risikolos an die jeweiligen Bedürfnisse anpassen.

bb) Erläutern Sie ein Problem, das hinsichtlich des Datenschutzes besonders in Cloud-Systemen auftritt. (2 Punkten)

Cloud-Services sind durch ihre Exponiertheit im Internet zahlreichen Angriffsmöglichkeiten und Gefahren ausgesetzt. Sie sind öffentlich erreichbar und zumeist betreiben Dritte ihre Infrastruktur, was beides Sicherheitsrisiken zur Folge hat.

Die [Cloud Security Alliance (CSA)](https://cloudsecurityalliance.org/) hat die aus ihrer Sicht größten Gefahren bei der Nutzung von (Public) [Cloud Computing](http://www.computerwoche.de/k/cloud-computing,3454) beschrieben:

* **Missbrauch und schädliche Nutzung von Cloud Computing**

Begünstigt durch grundlegende Eigenschaften von Cloud-Infrastrukturen (wie die schnelle und einfache Verfügbarkeit neuer Ressourcen mit sehr guter Netzanbindung) ist die Nutzung von Cloud-Ressourcen für Angreifer sehr interessant, um beispielsweise [Denial-of-Service-Attacken (DoS)](http://www.computerwoche.de/security/2504910/) zu starten oder Schadsoftware zu hosten.

* **Unsichere Schnittstellen und APIs**

Cloud-Services und die von den Anbietern zur Verfügung gestellten Management-Schnittstellen sind bei Public-Cloud-Angeboten über das Internet erreichbar und lassen sich daher leicht angreifen. Darüber hinaus existieren Programmierschnittstellen, die von den Anwendern zur Steuerung und Konfiguration der Cloud-Services verwendet werden können. Schwachstellen an diesen Interfaces öffnen möglicherweise Einfallstore, um beispielsweise unrechtmäßigen Zugriff auf Kundendaten zu erhalten.

* **Böswillige Insider**

Sicherheitsmaßnahmen der Software sind oft wirkungslos, wenn der Angreifer auf die Infrastruktur des Cloud-Anbieters zugreifen kann. Das ist besonders bei böswilligen Insidern der Fall - also Mitarbeitern des Cloud-Anbieters, die sich Zugriff auf Kundendaten verschaffen.

* **Risiken durch geteilte Technologien**

Eine weitere Eigenschaft von Cloud Computing ist das so genannte Pooling von Ressourcen. Das bedeutet, dass die physischen Ressourcen von allen Anwendern der Cloud-Services gemeinsam verwendet werden. Dabei können sich Probleme bei der zuverlässigen Trennung der Nutzerdaten ergeben.

* **Datenverlust und -kompromittierung**

Weil die Daten in der Cloud gespeichert sind und viele Anwender gleichzeitig dieselbe Infrastruktur verwenden, ergeben sich besondere Anforderungen an die Datensicherheit. Vergangene Probleme bei Cloud-Providern zeigen, dass es auch durch technische Probleme zu [Datenverlusten](http://www.computerwoche.de/security/2523112/) kommen kann.

* **Diebstahl von Benutzerkonten oder Cloud-Diensten**

Damit Anwender ihre Dienste schnell und einfach benutzen können, setzen viele [Cloud-Anbieter](http://www.computerwoche.de/security/2363866/index2.html) auf einen simplen Anmeldeprozess. Gelingt es einem Angreifer, die Zugangsdaten eines Kundenkontos in Erfahrung zu bringen, kann er unter falschem Namen auf fremde Daten zugreifen, Ressourcen missbrauchen und Schaden anrichten.