Technische Hochschule Ingolstadt

Professionelle Textsatzsysteme: Konzeptionierung einer Cloud-Infrastruktur im Mittelstand im Kontext von Secuirty und der Datenschutzgrundverordnung

Stefan Prieschl

4. Juli 2020

Erstprüfer Prof. Dr. Paul Spannaus
Zweitprüfer Christoph Nebl

Zusammenfassung

In der heutigen Zeit müssen Datensysteme immer mehr vernetzt werden, um einen globalen Arbeitskreislauf garantieren zu können. In diesem Bereich haben sich große Cloud-Anbieter etabliert, welche günstige Preise und unschlagbare Datensicherheit versprechen. Jedoch kann es für hohe Datenmengen sehr schnell sehr teuer werden. Hier kann sich ein eigener Server mit der dementsprechenden Ausstattung rechnen. Neben dem Preis gibt es allerdings noch weitere Faktoren, welche die Wahl der richtigen Lösung zur sicheren Datenspeicherung beeinflussen sollten.

1 Einleitung

1.1 Motivation

Die Motivation dieser Arbeit besteht darin, kleinen und mittelständischen Unternehmen zu helfen, sich für eine maßgeschneiderte Cloud-Lösung für die Firmendaten zu entscheiden. Die wichtigsten Punkte hierbei sind die monatlichen bzw. einmaligen Kosten, die Sicherheit gegen Datenverlust sowie die Datenschutzkonformität. Dieses Arbeit ist vor allem für Unternehmen gedacht, welche noch keine passable Lösung für die Datenspeicherung besitzen. Es werden explizit keine Software- und Hardwarehersteller genannt. Leider gibt es zu vielen Punkten wenig Literatur, wodurch viele Aussagen aus persönlicher Erfahrung in diesem Bereich resultieren.

1.2 Stand der Technik

In unserer vernetzten Welt ist es auch für kleine Betriebe unerlässlich, ihre Daten sicher abzuspeichern, da es bei einem Datenverlust zu hohen finanziellen Einbußen kommen kann. In Zeiten von Home-Office und weltweit verteilten Firmenstandorten ist es wichtig diese Daten möglichst schnell, auch über das Internet, zu erreichen und damit arbeiten zu können. Hierfür eigenen sich Cloud-Lösungen bestens. Für das Speichern personenbezogener Daten von EU-Bürgern muss außerdem die Datenschutzgrundverordnung eingehalten werden, da sonst empfindliche Strafen drohen.[1] Für viele, vor allem kleine Unternehmen, ist jedoch die Anschaffung von sicheren Speichermöglichkeiten entscheidend von der Kostenfrage abhängig. Hier ist es je nach Datenmenge und Anbindung des Betriebes entscheidend, ob sich auf lange Sicht eher eine fertige Lösung eines großen Cloud-Anbieters lohnt oder ob es sinnvoller ist, dass sich das Unternehmen selbst die nötige Hardware besorgt und verwaltet.

1.3 Begriffserklärung Cloud

Als Cloud wird die Auslagerung von IT-Recourcen ins Internet bezeichnet.[2, S.1] Der Oberbegriff IT-Resourcen beinhaltet sowohl Speicher als auch Rechenleistung. Hier kann grundsätzlich zwischen einer persönlichen Cloud, welche selbst betrieben wird und einer öffentlichen Cloud, welche von einem Anbieter betrieben wird, unterschieden werden. [3]

1.4 DSGVO

Seit dem Inkrafttreten der Datenschutzgrundverordnung in Europa am 25.05.2018 [1] müssen für die Speicherung und Verarbeitung personenbezogener Daten von EU-Bürgern bestimmte Voraussetzungen eingehalten werden. So dürfen personenbezogene Daten nach Art. 45 DSGVO[1] nur ins nicht EU-Ausland übertragen werden, wenn das Land gleichwertige oder höhere Datenschutzstandards bietet. Länder wie die USA und China bieten einen solchen Datenschutz nicht. Hier muss der Cloud-Anbieter nachweisen, dass die Daten datenschutzrechtlich korrekt gespeichert werden. Alternativ ist hier auch eine komplette Verschlüsselung der Daten zu erwägen. Zur Sicherstellung der Datenschutzkonformitiät muss ein Datenschutzbeauftragter nach Art. 37 DSGVO[1] abgestellt werden. Auch muss der Kunde welcher Daten abgibt nach Art. 12 DSGVO[1] transparent über den Verwendungszweck und seiner Verarbeitung informiert werden. Bei Zuwiderhandlungen können sonst nach Art. 83 Abs. 5 DSGVO[1] bis zu 20 Mio. Euro oder bis zu 4% des Jahresumsatzes als Strafe gefordert werden.

2 Wahl der richtigen Cloud

Dieses Kapitel soll helfen, sich zwischen einer öffentlichen Cloud oder einer selbst gehosteten privaten Cloud zu entscheiden.

2.1 Kosten

Die Preisgestaltung zwischen öffentlicher Cloud, wie z.B. die Amazon AWS Cloud und einer eigenen Cloud, z.B. ein Network Attached Storage (NAS)-System unterscheidet sich grundlegend. Bei einer öffentlichen Cloud wird meist ein Preis pro GB an gespeicherten Daten sowie eine Transfergebühr für das übertragen im Internet erhoben. Alternativ bieten viele Betreiber von öffentlichen Clouds noch nutzerbasierte Lösungen. Hier wird ein Preis für jeden Benutzer und deren zugewiesene Speichergröße zugeteilt, die Datenübertragung ist hier aber gratis im Paket enthalten. [4] [5] [6] [7] Bei einer eigenen Cloudlösung sind die hohen Anschaffungskosten für das Gerät selbst, die verwendeten Speichermedien sowie Speicher für das Backup zu beachten. Jedoch beinhalten die monatlichen Kosten nur den Preis für den verbrauchten Strom. Wie in der Tabelle 2.1 zu erkennen ist, lohnt es sich für große Datenmengen oder viele Benutzer nicht, eine öffentliche Cloud-Lösung zu nutzen, sofern die Internetanbindung nach draußen schnell genug ist.

Um zu berechnen, wie lange es dauert, bis die private Cloud günstiger als eine öffentliche Cloud ist, kann folgende Formel verwendet werden: Die Hardwarekosten ergeben sich aus dem Preis für den Hauptserver mit Speicher sowie den Kosten für das Backup. Die Stromkosten beziehen sich auf den monatlich verbrauchten Strom für die eigene Cloud-Lösung.

$$t = \frac{Hardwarekosten}{Monatspreis\,Cloud - Stromkosten}$$

Liegt dieser Wert unter der Garantiezeit der Hardware, lohnt sich aus finanzieller Sicht ein eigenes System (ohne Einrichtungskosten durch Dienstleister).

2.2 Internetanbindung

Ein einschränkendes Thema beim arbeiten mit Cloud-Lösungen, ist die in Deutschland an vielen Standorten immer noch schlechte Internetverbindung. So sind deutschlandweit 20,9% [8, S. 15] der Unternehmen noch mit unter 100 Mbit versorgt und damit nur eingeschränkt cloudfähig. 13,5% [8, S. 15] der Unternehmen sind mit unter 50 Mbit versorgt und somit überhaupt nicht für das Arbeiten in der Cloud geeignet. Um dieses Problem zu minimieren, haben je nach Firmenkonstellation, die öffentliche sowie die private Cloud jeweils ihre Vor- und Nachteile. Die folgenden zwei Grafiken zeigen den Unterschied zwischen öffentlicher und privater Cloud. Bei langsamen Internetanbindungen besteht das Ziel darin, die Menge der Daten, welche über den Internetanschluss laufen zu minimieren.

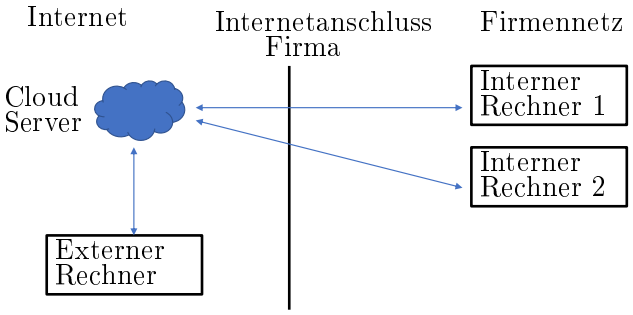

Abbildung 2.1: Aufbau einer öffentlichen Cloud: Alle Datenübertragungen der internen Rechner müssen über die Internetverbindung der Firma laufen. Sinnvoll, wenn Mitarbeiter überwiegend von Standorten außerhalb der Firma arbeiten.

Anbieter	Preis Speicher	Preis Übertragung	Abrechnung
Amazon AWS S3	0,0045 USD pro GB	0,036 USD pro GB	monatlicht
Google BigQuery	0.020 USD pro GB	0,005 USD pro GB	monatlich
Amazon Cloud Drive	99,99 € pro TB	gratis	jährlich
Google Drive Business	8 USD pro User + 1 USD pro 25GB	gratis	monatlich
Eigene Cloud 4 TB + Backup	1900 € (475 € pro TB)	gratis	einmalig
Eigene Cloud 8 TB + Backup	2140 € (267,5 € pro TB)	gratis	einmalig
Eigene Cloud 28 TB + Backup	4700 € (167,8 € pro TB)	gratis	einmalig

Tabelle 2.1: Preisübersicht Anbieter [4] [5] [6] [7], eigene Cloud Beispielrechnung NAS-System + 4 Festplatten Raid 6 - Backup besteht aus identischem System.

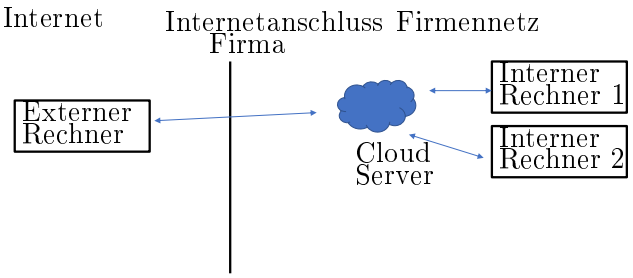

Abbildung 2.2: Aufbau einer privaten Cloud: Alle Datenübertragungen der internen Rechner erfolgen über ein lokales Netz. Sinnvoll, wenn überwiegend in der Firma mit den Daten gearbeitet wird.

2.3 Datensicherheit und Backup

Es gibt keine Sicherheit gegen Datenverlust, wenn kein Backup erstellt wird. Bei den bekannten Cloud Anbietern werden hierfür die Daten mehrfach auf den weltweit verteilten Servern gespeichert. Bei einer eigenen Cloud muss das Backup selbst verwaltet werden. Hier kommen zusätzliche Kosten für die Backupmedien hinzu.

2.4 Skalierbarkeit

Der wohl größte Vorteil von öffentlichen Cloud-Lösungen besteht in der einfachen und schnellen Skalierbarkeit der Anwendung. Wird mehr Speicher benötigt, kann dieser einfach hinzu gebucht werden. Bei privaten Cloud-Lösungen muss hingegen Hardware geordert, eingebaut und verwaltet werden. Hier sind keine schnellen Skalierungen möglich.

2.5 Privatsphäre

Werden bei öffentlichen Cloud-Anbietern unverschlüsselt Daten hochgeladen, muss dem Anbieter vertraut werden, die Daten für sich und andere unlesbar zu speichern. Hierbei ist es in der Vergangenheit bereits zu mehreren Datenleaks gekommen. Die eigene Cloud bietet hier allerdings auch keinen gänzlichen Schutz, wenn diese nicht richtig konfiguriert oder die Mitarbeiter mit der Anwendung fahrlässig handeln.

2.6 Verwaltungsaufwand

Bei öffentlichen Cloud-Lösungen kümmert sich der Betreiber um die Verwaltung der Hard- und Software. Der Aufwand für die eigene Cloud darf nicht unterschätzt werden und kann auch zusätzliche Kosten verursachen, wenn diese von einem Dienstleister verwaltet wird. Wenn genügend Know-How in der Firma vorhanden ist, stellt dieser Punkt kein Problem dar.

2.7 Entscheidung treffen

Je nachdem welche Parameter bezüglich Internetgeschwindigkeit und Speichermenge gegeben sind, ist es notwendig, die richtige Lösung für das Unternehmen zu finden. Bei hohen Datenmengen lohnt sich eigene Hardware bereits nach kurzer Zeit. Sind dagegen nur geringe Datenmengen auf wenigen Anwendern vorhanden oder das Wissen über die Einrichtung nicht gegeben, so kann es vorteilhaft sein, sich bei einem der bekannten Anbieter einzumieten.

3 Eigene Cloud einrichten

Wenn im vorherigen Kapitel die Vorzüge der eigenen Cloud für ihr Unternehmen überwiegen, wird hier die mögliche Konfiguration gezeigt:

3.1 Die richtige Hardware

Abhängig von der Datenmenge und der benötigten Geschwindigkeit ist es wichtig, die richtige Lösung für das Unternehmen zu finden. Dies kann für einfache Verwaltung und geringen Stromverbrauch ein fertiges NAS-System sein. Es kann aber auch bei Ansprüchen in den Peterbyte-Bereich ein Servercluster mit der dementsprechenden Software sein. Werden sehr hohe Datenraten über dem momentanen Standard von 1GBit benötigt, muss zusätzlich in dementsprechende Netzwerkhardware investiert werden. So müssen sowohl der Server, die Switche und nicht zuletzt der Endrechner dementsprechende Netzwerkgeschwindigkeiten unterstützen. Soll es ein einfaches NAS-System sein, sollte darauf geachtet werden, ein Gerät mit x86 Prozessor zu kaufen, da diese meistens mehr Leistung sowie eine bessere Unterstützung für Drittanbietersoftware bieten.

3.2 Die richtige Sofware

Das richtige Betriebssystem für den Server entscheidet, welche Funktionen später unterstützt werden. Fertige NAS-Systeme haben hier meist eine herstellereigene Software, welche sehr einfach zu konfigurieren ist, jedoch beim Funktionsumfang nur durch die Programme erweitert werden kann, welche im App-Store des Herstellers erhältlich sind. Dies deckt meist Programme für Samba-Shares (Netzwerklaufwerk in Windows Netzwerk), Virtual-Private-Network-(VPN)Software, um den Server und das Firmennetz von außerhalb zu erreichen und Backup Software ab. Unterstützt das NAS hingegen sogenannte Docker Container, kann auf eine schier endlose Menge von Programmen aus dem Docker Hub zugegriffen werden. Dies sollte für die meisten kleineren Unternehmen reichen. Wird ein richtiger Server zum Einsatz gebracht, kann von einer Vielzahl, zum Teil auch kostenloser Software Gebrauch gemacht werden.

3.3 Updates

Für die Datensicherheit ist es stets notwendig, das System auf einem aktuellen Stand zu halten. Hier ist es sinnvoll, alle Softwarekomponenten, welche mit dem Internet kommunizieren, per manuellen oder automatischen Update nach Betriebsschluss zu aktualisieren. Dies führt natürlich zu einem höheren Verwaltungsaufwand.

3.4 Erreichbarkeit aus dem Internet

Die Erreichbarkeit über das Internet kann über mehrere Wege erfolgen. Der Einfachste und Sicherste ist das Einrichten eines VPN-Netzwerkes, welches einen verschlüsselten Zugang zum Firmennetz darstellt. Hierfür gibt es ebenfalls die Möglichkeit den VPN Server auf dem Speicherserver zu installieren. Die zweite Methode besteht in der Verwendung einer Cloud-Software in Kombination mit einem Reverse-Proxy, welcher die Verschlüsselung per SSL sicherstellt. Hier gibt es dann die Möglichkeit, nach einer Anmeldung der Firmendomain die eigene Cloud über jeden Webbrowser über die gewählte URL, z.B. www.file.<Firmenname>.de zu erreichen. Hieraus können dann meist auch Links auf ganze Ordner oder Objekte erstellt werden, welche mit Externen geteilt werden können. Dies erleichtert den Austausch großer Daten enorm.

3.5 Die richtigen Speichermedien

Nachdem der Server bzw. das NAS-System gewählt wurde, müssen noch die richtigen Laufwerke für die Anwendung gefunden werden. Dies können große und günstige Festplatten, welche für den Dauerbetrieb ausgelegt sind (diese werden von den Herstellern als NAS oder Enterprise Festplatten bezeichnet) oder bei hohen Geschwindigkeitsansprüchen auch SSDs sein, welche allerdings pro GB noch sehr viel teurer sind. Hier ist je nach verwendeter Software auch ein Mischbetrieb möglich, sodass z.B. die SSD(s) als schneller Zwischenspeicher verwendet werden können.

3.6 Datensicherung

Auch wenn ein Raid (siehe Kapitel 3.10) eingerichtet wird, sind die Daten damit nicht gegen Datenverlust sicher, so kann es z.B bei Umweltkatastrophen, welche sich auf den Standort des privaten Cloud-Servers auswirken, zu einem Totalausfall kommen. Auch Viren, wie z.B. Verschlüsselungstrojaner, können den kompletten Datenbestand zerstören, wenn sie auf einem Rechner mit Zugriff auf den Cloud-Speicher ausgeführt werden. Somit ist es wichtig, mindestens ein aktuelles Backup zu haben, welches örtlich getrennt vom Firmenstandort gelagert wird. Bei wenigen Daten können dies zwei große Festplatten sein, welche abwechselnd per USB an den Server angeschlossen und das System darauf gespiegelt wird. Im Anschluss wird die Festplatte z.B. in der Wohnung des Geschäftsführers gelagert und mit der zweiten Festplatte am nächsten Tag genauso vorgegangen. Hierzu haben die meisten NAS-Systeme eine eingebaute Backupmöglichkeit, welche auch inkrementelle Backups zulässt, wodurch auf den Datenstand eines jeden Tages zugegriffen werden kann. Hier muss jedoch darauf geachtet werden, dass die Festplatte verschlüsselt wird, um zu garantieren, dass bei einem Verlust keine Firmendaten lesbar sind. Wenn die Datenmengen größer sind, ist es sinnvoll, an einem zweiten Standort einen Backup-Server einzurichten, welcher die Datensicherung inkrementell durchführt. Auch hier haben die meisten fertigen NAS-Systeme eine eingebaute Software, womit die Daten verschlüsselt zum Backup übertragen werden. [9] Bei extrem hohen Datenmengen kann sich die Besorgung eines LTO-Bandlaufwerkes lohnen, da nach der Investition des sehr teuren Laufwerkes, die Speichermedien selbst extrem günstig sind und eine Haltbarkeit bis zu 30 Jahre versprechen.[10]

3.7 Synchronisation oder Netzwerklaufwerk

Bei der Einbindung von Cloud-Speicher bestehen grundlegend zwei Möglichkeiten: Entweder wird der Speicher als Netzwerklaufwerk verbunden, d.h. er fungiert wie ein Laufwerk am Rechner, welches allerdings nur bei bestehender Anbindung an den Server benötigte Dateien zur Verfügung stellen kann. Die zweite Methode ist das Synchronisieren aller Daten des Benutzers auf den lokalen Rechner, dies bietet den Vorteil, dass die Dateien auch im Offline Zustand zur Verfügung stehen. Jedoch muss auf den Arbeitsrechner des Mitarbeiters auch so viel Speicherplatz zur Verfügung stehen, um die benötigten Dateien zu beherbergen. Hierfür muss spezielle Software auf dem Server und auf den Arbeitsrechnern installiert werden. Grundlegend kann gesagt werden, wenn sich der Datensatz in absehbarer Zeit im Rahmen hält, ist die Datensynchronisation ein gutes Mittel. Bei Speichergrößen im Terabyte Bereich, wenn z.B. große Video- oder Bildbestände vorhanden sind, ist es dagegen sinnvoller ein Netzwerklaufwerk zu verwenden.

3.8 Dateiversionierung

Um versehentliche Änderungen an Dateien wieder zurücksetzen zu können, empfiehlt sich die Aktivierung einer Dateiversionierung, wenn dies auf der Serversoftware möglich ist. Hiermit werden alle Änderungen an der Datei als Verlauf gespeichert, wodurch wieder auf einen früheren Standpunkt zurück gegangen werden kann. Auch ist es sinnvoll, sich einen Papierkorb einzurichten, falls ein Netzwerklaufwerk verwendet wird. Standardmäßig sind hier die Dateien einfach weg wenn man sie löscht. Ansonsten müsste immer

das Backup herbeigezogen werden, um versehentlich gelöschte Dateien wiederherzustellen.

3.9 Auslagerung in Rechenzentrum

Reicht die eigene Internetkapaziät nicht für den Upload großer Datenmengen aus, kann der Server in ein externes Rechenzentrum mit starker Anbindung verlagert werden, hier kommen monatliche Kosten für die Miete hinzu. Dies lohnt sich nur bei großen Datenmengen im Vergleich zur öffentlichen Cloud.

3.10 Das richige Raid-Level

Um mehrere Festplatten zu einem großen Laufwerk zu verbinden und Ausfallsicherheit gewährleisten zu können, wird in den meisten Fällen ein sogenanntes Raid aufgebaut. Je nach Raid-Level können während des Betriebes bis zu 2 Festplatten im Array ausfallen und die Daten durch einfaches tauschen der defekten Festplatten wiederhergestellt werden. Auch bei der besten Festplatte wird es früher oder später zu einem Ausfall kommen. Die Lese- und Schreibperformance kann je nach Implementierung des Raids abweichen. Hier die wichtigsten Raid-Versionen und deren Funktionsweise:

$$C = Kapazität$$

$$n = Anzahl\ Festplatten$$

$$d = Einzelkapazitaet\ Festplatte$$

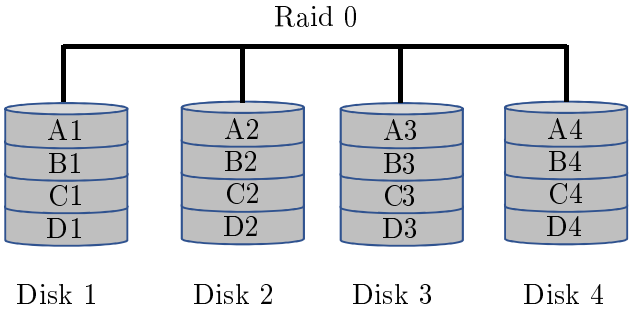

Abbildung 3.1: Raid0: Die Daten werden auf allen Platten verteilt: sehr schnell aber keine Sicherheit gegen einen Festplattenausfall. Sollte daher für wichtige Daten nicht verwendet werden.[11, S. 2]

$$C = n\,d$$

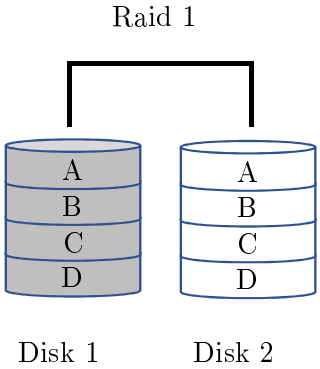

Abbildung 3.2: Raid1: Die Dateien werden auf 2 Festplatten gespiegelt: einfacher Schutz gegen Festplattenausfall, aber nicht besonders schnell.[11, S. 3]

$$C = \frac{n}{2}\,d$$

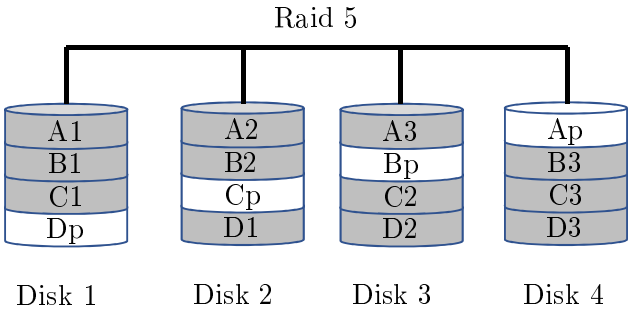

Abbildung 3.3: Raid5: Für alle Festplatten wird eine einfache Parität (Quersumme der Bits an gleicher Stelle auf den Laufwerken) gespeichert: einfache Redundanz, skaliert mit vielen Festplatten sehr gut.[11, S. 6]

$$C = (n-1)\,d$$

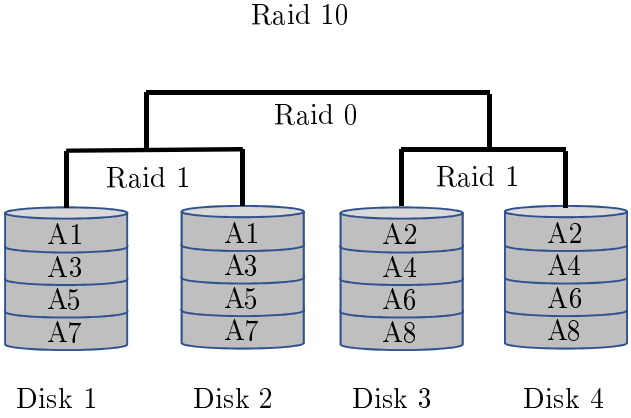

Abbildung 3.4: Raid10: Ein Raid0 wird über zwei Raid1 Systeme aufgespannt: doppelte Redundanz, wenn jeweils eine Festplatte per Raid1 ausfällt. [11, S. 10]

$$C = \frac{n}{2}\,d$$

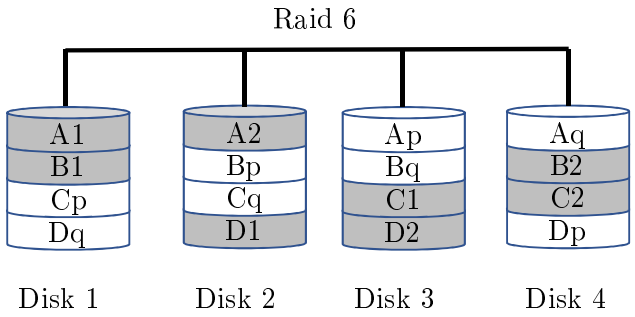

Abbildung 3.5: Raid6: Es werden 2 Paritäten mit unterschiedlichen Algorithmen erzeugt: doppelte Redundanz aber höherer Rechenaufwand. Es ist wichtig hier einen Server mit genügend Rechenleistung zu verwenden. [11, S. 8]

$$C = (n-2)\,d$$

Zusammenfassung und Empfehlung: Für ein gut zu verwaltendes System fallen Raid0 (3.1) wegen seiner Unsicherheit, sowie Raid1, (3.2) da es oft nicht über zwei Festplatten hinaus implementierbar ist, heraus. Raid5 (3.3) ist gut für einfache Sicherheit, hier kommt es aber nach einem Ausfall von zwei Festplatten definitiv zu einem Datenverlust. Hier kann es passieren, dass es nach dem Festplattentausch während des Wiederaufbaus der Daten durch die erhöhte Beanspruchung über mehrere Stunden zu einem Ausfall einer zweiten Festplatte kommt. Hier bietet Raid6 (3.5) einen besseren Schutz, da es einen zweifachen Festplattenausfall verkraften kann. Durch die zweite Paritätsberechnung, welche nicht nur eine einfache Quersumme darstellt, muss der Raid-Controller bzw. die CPU des Servers wesentlich mehr berechnen. Dies kann bei schlechter Hardware zu einer deutlich langsameren Schreibleistung kommen. Wenn maximale Leistung benötigt wird, eignet sich hierzu ein Raid10 (3.4) am besten. Es müssen keine Paritäten berechnet werden, wodurch die Schreibleistung bei nahezu jeder Serverhardware nur durch Leistung der Laufwerke begrenzt wird.

4 öffentliche Cloud einrichten

Wenn im Kapitel 2 die Vorzüge der öffentlichen Cloud überwiegen, oder einfach das technische Wissen für eine eigene Implementierung nicht vorhanden ist, soll dieses Kapitel weiterhelfen.

4.1 Anbieter finden

Bei der Wahl des Anbieters sollte man auf unabhängige Prüfungen achten, damit sichergestellt werden kann, dass der Anbieter DSGVO-Konform handelt. Erst wenn dieses Merkmal gegeben ist, sollte der Anbieter nach den Preis ausgewählt werden.

4.2 Die richtige Datenmenge kaufen

Da stets mehr Speicher zugekauft werden kann, ist es sinnvoll am Anfang nur die minimal nötige Menge zu kaufen, und bei Bedarf nachzukaufen. Einige Anbieter haben hier die Möglichkeit, die Speichermenge und somit die laufenden Kosten automatisch anzupassen. [7]

4.3 Installation ohne Verschlüsselung

Sollen die Daten nicht vor dem Hochladen bereits verschlüsselt werden, kann einfach die Software des Anbieters verwendet werden, um die Cloud mit den Geräten wie Computer und Smartphones zu verbinden.

4.4 Installation mit Verschlüsselung

Soll hingegen sichergestellt werden, dass die Daten auf der Cloud nicht für Dritte lesbar sind, bieten einige Cloud Anbieter eine Funktion an, dies per Verschlüsselung auf dem Cloud-Server zu ermöglichen. Sollen die Daten hingegen bereits vor dem Hochladen verschlüsselt werden, so muss meist eine Drittanbietersoftware verwendet werden. [12] Hier gibt es auch Software, welche direkt mit den Cloud-Anbietern kommuniziert und die Daten, ohne dass es der Nutzer merkt, im Hintergrund verschlüsselt und dann erst beim Anbieter ablegt. Bei verschlüsselten Daten kann es jedoch zu Problemen mit Geräten kommen, welche die Software für die Entschlüsselung nicht unterstützen. Da die Dateien über einen Schlüssel verschlüsselt werden, ohne den nicht mehr entschlüsselt werden kann, ist es zwingend nötig, diesen sicher zu speichern, da sonst alle Dateien unwiederbringlich verloren sind.

5 Fazit

Bei der Auswahl der richtigen Cloud für ein Unternehmen, müssen viele Parameter beachtet werden. Darum kann pauschal keine Aussage getroffen werden, welche Lösung empfohlen werden kann. Werden allerdings alle Parameter für die Entscheidung beachtet, sollte sich eine optimale Lösung herauskristallisieren. Die eigene private Cloud erzeugt hierbei natürlich einen höheren Aufwand, sowohl bei der Einrichtung, als auch bei der Verwaltung. Dafür kann hier bei großen Datenmengen auf lange Zeit Kosten gespart werden. Werden nur geringe Mengen an Speicherplatz oder eine schnelle Verbindung an externe Mitarbeiter benötigt, kann sich eine öffentliche Cloud der großen Anbieter lohnen. In jedem Fall muss auf ein ausreichendes Backup geachtet werden. Hier empfiehlt sich das Speichern auf mindestens zwei Medien, wobei hier eines örtlich getrennt von der eigenen Cloud aufbewahrt werden sollte. Dieses sollte im besten Fall nicht nicht immer mit dem Internet verbunden sein, um Hackerangriffe zu vermeiden. Natürlich ist bei der Datenhaltung auch ein Mischbetrieb zwischen öffentlicher und privater Cloud möglich.

Literatur

[1] Europäische Union. *Datenschutz-Grundverordnung [online]: DSGVO*. 27.04.2016 [Zugriff am 04.07.2020]. URL: https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf.

[2] Dominic Lindner, Paul Niebler und Markus Wenzel. *Der Weg in die Cloud [online]: Ein Leitfaden für Unternehmer und Entscheider*. 1st ed. 2020. essentials. 2020 [Zugriff am 04.07.2020]. ISBN: 9783658291013. DOI: 10.1007/978-3-658-29101-3.

[3] Fraunhofer-Allianz Cloud Computing. *Was bedeutet Public, Private und Hybrid Cloud? [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://www.cloud.fraunhofer.de/de/faq/publicprivatehybrid.html.

[4] Amazon. *Amazon Drive Kosten [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://www.amazon.de/photos/storage/plans.

[5] Amazon. *Amazon S3 – Preise [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://aws.amazon.com/de/s3/pricing/.

[6] Google. *Google Drive Business Preise [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://cloud.google.com/drive-enterprise?hl=de#pricing.

[7] Google Cloud. *Google Big Query Preis [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://cloud.google.com/bigquery/pricing?hl=de.

[8] Bundesministerium für Verkehr und digitale Infrastruktur. *Bericht zum Breitbandatlas Teil1: Ergebnisse [online]*. 6.2019 [Zugriff am 04.07.2020]. URL: https://www.bmvi.de/SharedDocs/DE/Anlage/DG/Digitales/bericht-zum-breitbandatlas-mitte-2019-ergebnisse.pdf?__blob=publicationFile.

[9] Synology. *Synology Hyper Backup [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://www.synology.com/de-de/dsm/feature/hyper_backup.

[10] Arnon Amir u. a. „File-based media workflows using ltfs tapes [online]“. In: *Proceedings of the international conference on Multimedia [online]*. Hrsg. von Alberto del Bimbo. New York, NY: ACM, 2010 [Zugriff am 04.07.2020], S. 1519. ISBN: 9781605589336. DOI: 10.1145/1873951.1874269.

[11] Lacie. *LaCie Raid Technology White Paper [online]*. [Zugriff am 04.07.2020]. URL: https://www.lacie.com/files/lacie-content/whitepaper/WP_RAID_EN.pdf.

[12] Google Cloud. *Datenverschlüsselungsoptionen [online]*. 2020 [Zugriff am 04.07.2020]. URL: https://cloud.google.com/storage/docs/encryption.