

Machbarkeitsstudie zum Ersatz von lokalen Servern durch webgehostete Services in Kleinstunternehmen

Bachelorarbeit

eingereicht von: **Mag. rer. nat. Georg Grüner**
Matrikelnummer: 00949044

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades eines
Bachelor of Arts in Business

Betreuung und Beurteilung: DI Eszter Geresics-Földi MSc, BSc

Wiener Neustadt, Februar 2025

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Winzendorf, 11.02.2025



Unterschrift

Creative Commons Lizenz

Das Urheberrecht der vorliegenden Arbeit liegt bei Mag. Georg Grüner. Sofern nicht anders angegeben, sind die Inhalte unter einer Creative Commons „Creative Commons Namensnennung-Nicht kommerziell 4.0 International“ (CC BY-NC 4.0) lizenziert. Die Rechte an zitierten Abbildungen liegen bei den in der jeweiligen Quellenangabe genannten Urheber*innen.

Die Kapitel 1-2 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 10.2.2025 als Bachelorarbeit 1 angenommen.

Kurzzusammenfassung:

Machbarkeitsstudie zum Ersatz von lokalen Servern durch
webgehostete Services in Kleinstunternehmen

Diese Arbeit prüft die Umsetzbarkeit eines Wechsels von lokalen Servern zu Web-Diensten in kleinen Firmen bzw. in einem Kleinstunternehmen. Das Ziel liegt in der Untersuchung der technischen und wirtschaftlichen Aspekte sowie der Organisation und des Datenschutzes. Ausgehend vom Problem der teuren lokalen Server mit hohem Wartungsaufwand, stellt sich die zentrale Frage ob Web-Dienste und Online-Services eine brauchbare Alternative anbieten, um den Betrieb günstiger und ressourcenschonender am Laufen zu halten. Die Untersuchung nutzt: eine technische Analyse der Systemvoraussetzungen, eine Kostenbewertung von Investitionen als auch Betrieb und eine Prüfung der Umsetzung. Die Ergebnisse belegen viele Vorteile von Web-Diensten wie bessere Skalierbarkeit, niedrige Startkosten und Einhaltung des Datenschutzes. Hürden, u.A. die Anforderung einer gut funktionierenden (Grund-)Infrastruktur sowie der Anpassung aktueller Abläufe, wurden ebenfalls erkannt und bewertet. Ein Wechsel zu Web-Diensten stellt für kleine Firmen eine sehr gute Option dar, wenn im Vorfeld die entsprechenden Vorbereitungen getroffen werden. Der Umstieg ermöglicht eine bessere Ressourcennutzung und Kosteneinsparungen über lange Sicht. Diese Machbarkeitsstudie liefert IT-Managern und Geschäftsinhabern eine Handreichung bzw. ein Konzept zur Umstellung, sowie eine Abwägung, ob eine Umstellung sinnvoll zu erachten ist.

Schlagwörter: Machbarkeitsstudie, Cloud-Services in Kleinstunternehmen, Ressourcenschonende Infrastruktur, Datenschutz, Auslagern von Diensten, Datenschutz in der Cloud

Abstract:

Feasibility study on replacing local servers with
web-hosted services in micro-enterprises

This study addresses the feasibility of the transition to web-based services from local servers for small enterprises, with a thorough analysis of technical, economic, organizational, and data security considerations. The paper addresses necessary infrastructure requirements, installed systems compatibility, and the procedure for attaining perfect integration with least disruption during the conversion process. Evidence highlights advantages of web-hosted solutions like enhanced scalability, reduced capital expenditure through subscription-based models, and enhanced data protection with GDPR adherence. Economic evaluation acknowledges cost savings on hardware acquisition expenses, maintenance expenses, and energy expenses, while organizational analysis identifies implementation planning, training personnel, and adaptation to new technologies. The research also emphasizes the importance of sound risk management practices, including sound backup procedures, careful monitoring, and frequent security audits, to maintain data integrity and business continuity. Small businesses, by availing themselves of web-hosted services, can make the best use of IT resources, optimize operational effectiveness, and gain more flexibility to respond to changing market conditions. This in-depth report provides actionable advice and a strategic guide for small businesses wishing to embrace the cloud, enabling them to align IT infrastructure with business goals and sidestep pitfalls.

Keywords: Web-Hosted Services, Small Enterprises, Feasibility Analysis, Data Security, GDPR Compliance

Inhaltsverzeichnis

EHRENWÖRTLICHE ERKLÄRUNG	II
INHALTSVERZEICHNIS	V
1. EINLEITUNG	1
1.1 Hintergrund und Motivation	1
1.2 Forschungsfrage & Hypothese	2
1.3 Zielsetzung der Arbeit & Methodik	3
1.4 Status Quo & Problemanalyse	3
2. THEORETISCHE GRUNDLAGEN	5
2.1 Definition & Aufgaben eines Servers	5
2.2 Anforderungen eines Servers & an das Netzwerk in einem Kleinstbetrieb	6
2.2.1 Topologie eines Netzwerkes eines Kleinstbetriebs	6
2.2.2 Netzwerkkomponenten	9
2.2.3 Server in Kleinstbetrieben	10
2.2.4 Lizenzierung	11
2.2.5 Datenschutz, Netzwerk- & Datensicherheit	12
2.3 Webgehostete Services	13
2.3.1 Entwicklung und Verbreitung webgehosteter Services	13
2.3.2 Funktionsumfang	14
2.3.3 Technische Voraussetzungen	15
2.3.4 Datenschutz & Datensicherheit	17
2.4 Vor- und Nachteile von lokalen Serversysteme und webgehosteten Services	17
2.4.1 Kosten	17
2.5 Zugriff & Zuverlässigkeit	18
2.5.1 Implementierungszeit & Anpassungsmöglichkeiten	18
2.5.2 Datenschutz & Sicherheit	19
2.5.3 Zusammenfassung / Tabellarische Ansicht	21
2.6 Aktueller Forschungsstand	22
2.6.1 Digitalisierung und Cloud-Computing	22

2.6.2	Sicherheitsaspekte	22
2.6.3	Wirtschaftliche Überlegungen	23
2.6.4	Herausforderungen bei der Implementierung	23
2.6.5	Zukunftsausblick	24
3.	MACHBARKEITSSTUDIE	25
3.1	Technische Machbarkeit	25
3.1.1	Anforderungen an die Infrastruktur	25
3.1.2	Integration bestehender Systeme	27
3.1.3	Skalierbarkeit & Flexibilität	30
3.2	Wirtschaftliche Machbarkeit	33
3.2.1	Kostenanalyse & Vergleich	33
3.2.2	Investition & Betriebskosten	34
3.2.3	ROI-Betrachtung	34
3.3	Organisatorische Machbarkeit	36
3.3.1	Implementierungszeit & Aufwand	36
3.3.2	Schulungsbedarf & Ressourcen	37
3.3.3	Anpassbarkeit & Benutzerfreundlichkeit	38
4.	ANALYSE DATENSCHUTZ & DATENSICHERHEIT	40
4.1	Einhaltung der DSGVO	40
4.1.1	Grundlagen & Anforderungen	40
4.1.2	Betroffenenrechte & Transparenz	41
4.2	Sicherheitsstrategien & Maßnahmen	42
4.2.1	Verschlüsselung & Zugriffskontrollen	42
4.2.2	Netzwerksicherheit & Firewalls	43
4.3	Risikoanalyse & Schwachstellenbewertung	45
4.3.1	Identifikation & Bewertung von Risiken	45
4.3.2	Bedrohungsmodelle & Schutzmaßnahmen	46
4.4	Backup & Wiederherstellungsstrategien	48
4.4.1	Backup-Methoden & Speicherorte	48
4.4.2	Notfallwiederherstellung & Redundanz	50

5. AUSWERTUNG & ZUSAMMENFASSUNG DER ERGEBNISSE	52
6. BEANTWORTUNG DER FORSCHUNGSFRAGE	53
7. ZUSAMMENFASSUNG & AUSBLICK	54
GLOSSAR	55
LITERATURVERZEICHNIS	58
ABBILDUNGSVERZEICHNIS	64
TABELLENVERZEICHNIS	65

1. Einleitung

Die Digitalisierung wandelt die IT-Bedürfnisse von Kleinstunternehmen grundlegend um. Neue Herausforderungen entstehen besonders durch flexible Arbeitsformen wie Home-office oder Remote-Arbeit, aber auch an den lokalen Arbeitsplätzen. Diese benötigen IT-Lösungen, die sich durch Leistung Sicherheit sowie Wirtschaftlichkeit auszeichnen. Gerade an festen Standorten ist abzuwägen, ob lokale Investitionen wirtschaftlich vertretbar sind, oder ob eine Umstellung bzw. ein Wechsel auf webgehostete Services mehr Vorteile und zukünftige Potenziale für das Unternehmen bringt. Die Untersuchung prüft, ob sich webgehostete Dienste als Alternative zu lokalen Servern eignen. Dabei werden technische, wirtschaftliche als auch organisatorische Aspekte analysiert und bewertet.

1.1 Hintergrund und Motivation

Mit 99,6% aller Unternehmen zählen die KMUs (Klein- und Mittelunternehmen) zur größten Unternehmensgruppe in Österreich.¹ Bei rund 87% der KMUs handelt es sich um Kleinstbetriebe. Dies sind Großteils Ein-Personen-Betriebe (Einzelunternehmen) bzw. Betriebe mit maximal 10 Mitarbeiter. Fast alle Betriebe benötigen zur Durchführung ihrer Tätigkeiten eine entsprechende Infrastruktur bestehend aus Computer bzw. Notebooks und Internetanbindung, einige weitere benötigen zusätzlich Server und NAS-Systeme. Hier sind teilweise große Investitionen nötig, um mit der Geschäftstätigkeit überhaupt erst beginnen zu können.

In der heutigen digitalen Geschäftswelt sind leistungsfähige IT-Infrastrukturen für Unternehmen jeder Größe unverzichtbar. Auch Kleinstunternehmen, die meist nur über begrenzte personelle und finanzielle Ressourcen verfügen, stehen vor der Herausforderung, ihre IT effizient und sicher zu betreiben. Traditionell wird in vielen dieser Unternehmen auf lokale Serverlösungen zurückgegriffen, die jedoch hohe Investitionen in Hardware und Wartung erfordern und zudem zu erheblichen Sicherheitsrisiken führen können. Gleichzeitig bieten webgehostete Services, insbesondere Cloud-Lösungen, eine flexible und kostengünstige Alternative.

¹ BMDW, „Small and Medium Enterprises in Austria – Facts and Figures“, Bundesministerium für Arbeit und Wirtschaft, zugegriffen 30. Dezember 2024, <https://www.bmaw.gv.at/en/Topics/Business-Location/Small-and-medium-sized-Enterprises-SMEs/SME-in-Austria-facts-and-figures.html>.

Durch die Corona-Krise beschleunigt, wurden in den letzten Jahren zahlreiche webgehostete Services bereitgestellt.² Großteils wurden vorhandene lokal gehostete Serveranwendungen & -dienste in neueren Versionen webgehostet angeboten. Viele Unternehmen betreiben aber immer noch ihre lokalen Server, stehen aber demnächst vor der Entscheidung, diese zu erneuern, oder auch auf eine webgehostete Lösung umzusteigen.

Als selbstständiger Einzelunternehmer im Bereich Server- und Netzwerktechnik berate ich meine Kundinnen und Kunden bei der Modernisierung und Anpassung ihrer Systeme und versuche maßgeschneiderte Lösungen anzubieten. Hierbei lege ich Wert auf kostengünstige und einfache Lösungen, welche spezifisch auf das Anforderungsprofil des jeweiligen Kunden abgestimmt werden. Je nach Betrieb und Bedarf ist abzuwägen, welche Investitionen sinnvoll und in Relation zur Wirtschaftlichkeit des Unternehmens stehen. Weiters müssen je nach Betrieb zusätzliche Punkte bei der Planung und Umsetzung beachtet werden. Das klingt nach einer zukunftsorientierten Entscheidung, besonders angesichts der vielen Vorteile der Cloud, wie Skalierbarkeit und Flexibilität. Welche Art von Projekten plant man, bei denen externe Services einbezogen werden sollen.

1.2 Forschungsfrage & Hypothese

Forschungsfrage:

Ist es aus technischer, organisatorischer, wirtschaftlicher und datenschutzrechtlicher Sicht machbar, den lokalen Server eines Kleinunternehmens durch webgehostete Services zu ersetzen?

Hypothese:

Die Nutzung webgehosteter Services stellt eine effiziente und zukunftsichere Alternative zu lokalen Servern dar, insbesondere für Kleinunternehmen, die über begrenzte IT-Ressourcen verfügen. Durch die Integration von Cloud-Technologien können Betriebskosten gesenkt, Sicherheitsstandards verbessert und die Skalierbarkeit erhöht werden.

Erläuterung der Forschungsfrage:

Die zunehmende Digitalisierung und die wachsenden Anforderungen an flexible Arbeitsmodelle, wie Homeoffice und Remote-Arbeit, setzen die IT-Infrastrukturen von Kleinunternehmen zunehmend unter Druck. Diese Arbeit untersucht, ob webgehostete Services

² Jean-Michel Sahut und Raphael Lissillour, „The Adoption of Remote Work Platforms after the Covid-19 Lockdown: New Approach, New Evidence“, *Journal of Business Research* 154 (1. Januar 2023): 113345, <https://doi.org/10.1016/j.jbusres.2022.113345>.

eine bessere Lösung für die technischen, organisatorischen und wirtschaftlichen Herausforderungen dieser Unternehmen darstellen als herkömmliche lokale Serverlösungen, um auch auf das neue Arbeitsumfeld Rücksicht zu nehmen. Im Fokus stehen dabei verschiedene zentrale Gesichtspunkte: Die technische Machbarkeit wird anhand der Leistungsfähigkeit, Skalierbarkeit und Ausfallsicherheit von Cloud-Lösungen analysiert. Darüber hinaus erfolgt eine wirtschaftliche Bewertung der Kosten im Vergleich zu traditionellen Serverlösungen, um die langfristige Rentabilität zu bestimmen. Datenschutz und Sicherheit spielen eine wesentliche Rolle, weshalb die Einhaltung von DSGVO-Richtlinien und relevanten Sicherheitsstandards überprüft wird. Schließlich wird auch die organisatorische Integration betrachtet, insbesondere die Benutzerfreundlichkeit, der Wartungsaufwand sowie die vorhandenen Supportstrukturen.

Erläuterung der Hypothese:

Die Hypothese basiert auf der Annahme, dass webgehostete Services durch ihre Flexibilität und geringere Investitionskosten eine praktikable Lösung für Kleinunternehmen bieten. Diese Systeme ermöglichen eine schnelle Anpassung an neue Anforderungen und bieten hohe Sicherheitsstandards durch die Einhaltung aktueller Datenschutzvorgaben. Es wird erwartet, dass durch den Einsatz dieser Technologien die Produktivität gesteigert, die Wettbewerbsfähigkeit erhöht und der Wartungsaufwand verringert werden kann.

Diese Fragestellung und Hypothese bilden die Grundlage für die empirische Analyse dieser Machbarkeitsstudie.

1.3 Zielsetzung der Arbeit & Methodik

Diese Machbarkeitsstudie untersucht, ob es technisch, organisatorisch, wirtschaftlich und datenschutzrechtlich machbar ist, eine lokal betriebene Serverumgebung durch webgehostete Services zu ersetzen. Hierzu werden die Abläufe und Tätigkeiten eines lokalen Kleinunternehmens analysiert und die oben genannten Kriterien ausgearbeitet. Ziel dieser Arbeit ist es, klar herauszuarbeiten, ob ein 100% Umstieg zu externen Dienstleistern für den Betrieb sinnvoll und unter den genannten Punkten vertretbar ist. Dadurch soll eine fundierte Entscheidungsgrundlage für Kleinunternehmen geschaffen werden.

Hierbei stütze ich mein Fachwissen unter anderem auf Fachliteratur der Computer- und Netzwerktechnik, Erfahrungswerte sowie die Resultate einer bereits (teilweise) erfolgten Umstellung eines vergleichbaren Betriebs in vergleichbarer Größe.

1.4 Status Quo & Problemanalyse

Kleinunternehmen haben häufig begrenzte Mittel für IT-Investitionen. Die laufende Wartung lokaler Server, mögliche Ausfälle und die Notwendigkeit regelmäßiger Software-Updates führen oft zu hohen Betriebskosten und potenziellen Sicherheitslücken.

Die Problemanalyse untersucht die aktuellen Herausforderungen und beleuchtet, wie lokale Server im Vergleich zu Cloud-Lösungen abschneiden. Für die Lösung der Forschungsfrage wurde folgendes Szenario angenommen:

Ein lokales Kleinstunternehmen beschäftigt sechs Mitarbeiter und ist Bereich der Wirtschaftsprüfung und Steuerberatung tätig. Der Bürostandort beherbergt vier Arbeitsplätze. Betrieben wird eine lokale Serverumgebung, aufbauend auf einem Microsoft Windows 2012 R2 Server. Insgesamt gibt es fünf Clients (Notebooks), welche lokal verwaltet werden. Die benötigten Dateien werden zentral auf dem Server bereitgestellt. Zusätzlich können alle Mitarbeiter per VPN und Remote-Desktop-Verbindung auf einem Terminalserver zugreifen und auch im Homeoffice arbeiten. Die verwendete Hardware stammt Großteiles auf dem Jahr 2012 und ist leistungstechnisch an die Ihre Grenzen gestoßen. Das Serverbetriebssystem ist ans Ende des Supportzeitraums gelangt.³ Die verwendete Anwendungssoftware ist teils ebenfalls schon vier Jahre alt. Ein Upgrade ist aufgrund der technischen Voraussetzungen derzeit nicht möglich. Einzig die firmenspezifischen Programme (Buchhaltungssoftware, Lohnverrechnungsprogramm, ...) werden vom Hersteller noch unterstützt und ist aktuell.

Da eine Erneuerung der Hard- und Software aufgrund ihres hohen Alters und der damit verbundenen Sicherheitsrisiken unumgänglich ist, wurden Neuanschaffungen sowie konzeptionelle Änderungen in Betracht gezogen. Dabei wurden verschiedene Überlegungen angestellt, um eine fundierte Umrüstung zu ermöglichen. Zunächst wurde geprüft, ob Teile der vorhandenen Hardware weiterhin genutzt werden können und welche Software aktuell im Einsatz ist. Weiters wurde hinterfragt, ob eine eigene Serverumgebung überhaupt notwendig ist oder ob geeignete webgehostete Services die erforderlichen Funktionen des lokalen Servers übernehmen können. Basierend auf diesen Überlegungen wurde ein Konzept zur Integration und Überführung der bestehenden lokalen Serverumgebung auf eine webgehostete Alternative entwickelt. In der folgenden Arbeit wird dieser Entwurf detailliert ausgearbeitet und die technische, organisatorische, wirtschaftliche sowie datenschutzrechtliche Machbarkeit einer solchen Umstellung analysiert.

³ GitHub-Name, „Windows Server 2012 R2 - Microsoft Lifecycle“, zugegriffen 30. Dezember 2024, <https://learn.microsoft.com/de-de/lifecycle/products/windows-server-2012-r2>.

2. Theoretische Grundlagen

2.1 Definition & Aufgaben eines Servers

Ein Server (dt. Diener, Bediensteter) ist ein Computerprogramm bzw. ein Gerät, welcher den Arbeitsstationen (Clients) und Anwendern an zentraler Stelle Ressourcen und Funktionen zu Verfügung stellt.⁴ Die Clients nehmen seine Dienstleistungen hierbei in Anspruch (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**)⁵ Ein Server kann vielfältig ausgeprägt sein. Als z.B. reiner Fileserver, der Dateien im Netzwerk bereitstellt, als Druckserver, um gemeinsame Druckgeräte ressourcenschonend allen zur Verfügung zu stellen, als Datenbank-Server, um eine gemeinsame Datenbank verwenden zu können uvm. Heutzutage hat ein Server meist nicht nur eine Aufgabe, sondern mehrere gleichzeitig.

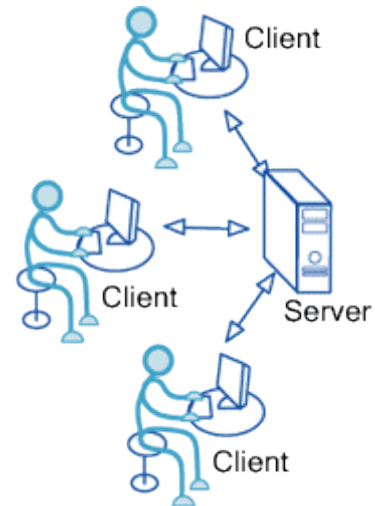


Abbildung 1: Server-Client Modell

In der Praxis werden mehrere Server gleichzeitig betrieben, um Redundanzen zu schaffen bzw. Dienste als eigenständige Serveranwendung abgekoppelt vom restlichen System laufen zu lassen. Dies kann physisch (jeder Server hat seine eigene Hardware) oder auch virtuell passieren und bietet den Vorteil an, dass bei einem Ausfall nicht alle Systeme betroffen sind.

Grundlage jeder Server-Client-Umgebung ist die Nutzung eines Domain Controllers (DC), welcher für die zentrale Authentifizierung von Computern und Benutzern im zuständig ist. Das schon 1970 von IBM entwickelte Konzept⁶ beruht auf einem vertrauenswürdigen, eigenständigen „Kontrollleur“ (Controller), welcher überprüft, ob Nutzer und Geräte einem Netzwerk beitreten dürfen. Der Begriff Domain bezieht sich hierbei auf den Netzwerknamen bzw. einem Bereich in einem physischen Netzwerk. Der Domain-Administrator ist nun in der Lage Benutzern und Geräten Zugriff auf einem administrativ abgegrenzten Netzwerkbereich zu gewähren und kann dies zentral über den Domain Controller steuern.

⁴ IT-Handbuch für Fachinformatiker: der Ausbildungsbegleiter, 7., aktualisierte und erweiterte Auflage 2015, 1. korrigierter Nachdruck 2016, Rheinwerk Computing (Bonn: Rheinwerk Verlag GmbH, 2016), 197.

⁵ „Client-Server“, Seite, zugegriffen 30. Dezember 2024, https://www.e-teaching.org/technik/vernetzung/architektur/client-server/index_html.

⁶ Peter Schmitz und Stefan Luber, „Was ist ein Domänencontroller?“, Security-Insider, 10. Februar 2021, <https://www.security-insider.de/was-ist-ein-domainencontroller-a-1021654/>.

Anfang der 1990ern wurde dieses Modell von Microsoft für Windows-Computernetzwerke unter dem Namen Aktive Directory Domain Services (ADDS) übernommen. Aufgrund des großen Marktanteils von über 70%⁷ von Windows Server Betriebssystemen, wurde ADDS schnell zum Standard für viele Firmennetzwerke. Das System zeichnet sich durch seine einfache Bedienbarkeit und Skalierbarkeit aus. Das Netzwerk wird nach den realen organisatorischen oder räumlichen Gegebenheiten des Unternehmens abgebildet und verhält sich ähnlich einer Zuordnungsliste bzw. einem Adressbuch. Kernelemente des ADDS sind unter anderen das *Lightweight Directory Access Protocol* (kurz: LDAP) sowie das *Domain Name System* (kurz: DNS). Beide Systeme sind RFC-standardisiert und bieten somit die Möglichkeit die Authentifizierungsfunktion des Microsoft-Server-Betriebssystems auch außerhalb der Windows-Welt zu nutzen. Somit ist es auch u.a. Linux und MacOS-Geräten möglich einen Windows-Server als Authentifizierungsserver zu nutzen.

2.2 Anforderungen eines Servers & an das Netzwerk in einem Kleinstbetrieb

Je nachdem, welche Programme, Services und Dienste genutzt werden, können die Anforderungen eines Servers im Netzwerk sowie die Struktur des Netzwerkes selbst variieren. Sinngemäß ist ein Netzwerk eine physische Infrastruktur, die Datenendgeräte eine wahlfreie Kommunikation, den Datenaustausch sowie die Nutzung gemeinsamer Ressourcen ermöglicht. So kann u. a. die Internetverbindung, der Drucker bzw. Kopierer gemeinsam genutzt als auch Daten an einem zentralen Datenspeicherort gelagert werden. In modernen Computernetzwerken gibt es keine exklusiven 1:1 Verbindungen, weshalb es bei Fehlern selten zum Totalausfällen kommt.⁸

2.2.1 Topologie eines Netzwerkes eines Kleinstbetriebs

Je nach Größe, Struktur und Anforderungen des Unternehmens muss die physische Verkabelung geplant und entsprechend aufgebaut werden. Die Topologie eines Computernetzwerkes beschreibt die physische Anordnung der Geräte und Leitungen in einem

⁷ „Betriebssysteme - Marktanteile weltweit 2024“, Statista, zugegriffen 30. Dezember 2024, <https://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/>.

⁸ Editorial Team, „Fault Tolerance“, Network Encyclopedia, 11. September 2019, <https://networkencyclopedia.com/fault-tolerance/>.

Computernetzwerk und stellt somit die Wege dar, die Daten von und zum Endgerät übertragen werden.⁹ Die Struktur eines Netzwerkes ist maßgeblich für deren Ausfallsicherheit und Performance und sollte auch bei der Budgetplanung berücksichtigt werden, da die benötigte Hardware entsprechend den Anforderungen angeschafft werden muss.

Abbildung 2 zeigt diverse Möglichkeiten wie Clients und Server miteinander verbunden werden können. Die Strukturen der vorgestellten Netzwerktopologien bieten Vor- und Nachteile für den Netzbetreiber:

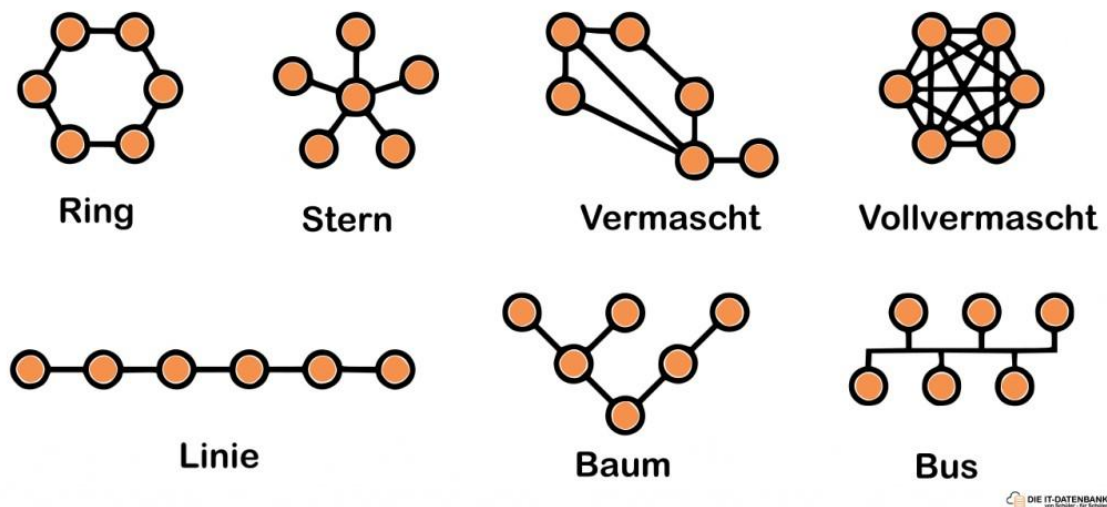


Abbildung 2: Netzwerktopologien¹⁰

Jeder Punkt im Netzwerk steht für ein Endgerät, ganz gleich ob Server, Client oder Resource. Jede dieser Anordnungen hat Vor- bzw. Nachteile bzw. sind teilweise historisch gewachsen. Prinzipiell kann jede dieser Anordnungen für eine Realisierung herangezogen werden, weshalb es einer weiteren Erklärung dieser Bedarf:

Linie- und Ring-Topologie sind veraltete Strukturen, welche auf die frühe Entwicklung der Computernetzwerke zurückgeht. Meist wurde die Vernetzung der Computer durch Koaxial-Kabel realisiert. Die Kosten für diese Anordnungen waren meist gering, da nur geringe Kabelmengen benötigt wurden und aufgrund der Einfachheit das Netzwerk sehr schnell erweitert werden konnte. Jedes Gerät gab die Informationen an das jeweils nächste weiter, weshalb stets alle Geräte aktiv sein mussten. Ein Ausfall bzw. eine Fehlfunktion eines Endgerätes hatte im Falle der Linie eine Unterbrechung zur Folge. In der

⁹ Qing Liu und Qiuping Liu, „A Study on Topology in Computer Network“, in *2014 7th International Conference on Intelligent Computation Technology and Automation*, 2014, 45–48, <https://doi.org/10.1109/ICICTA.2014.18>.

¹⁰ „Topologien – IT-Datenbank.com“, 29. August 2020, <https://it-datenbank.com/topologien/>.

Ring-Struktur wird als Ausfallssicherung der alternative Weg in die Gegenrichtung gesendet. Problematisch bei beiden Strukturen war der Datenstau, da aufgrund des geringen Datendurchsatzes von 10 Mbit/s und des stetigen „Weitergeben“ die Datenmengen nicht in angemessene Zeiten übergeben werden konnte.¹¹

Die BUS-Topologie verbindet alle Geräte über eine gemeinsame zentrale Verbindung. Um eine Vermischung der Datenpakete zu vermeiden, muss allerdings sichergestellt werden, dass immer nur ein Gerät zum jeweiligen Zeitpunkt sendet. Die Steuerung hierfür übernimmt ein BUS-Anbieter, der dem jeweiligen Client ein Zeitfenster für das Senden zur Verfügung stellt. Der Vorteil bei dieser Struktur ist u.a. die direkte und alleinige Kommunikation von Sender zum Empfänger und somit zur maximal möglichen Bandbreite sowie die Tatsache, dass nicht alle Clients aktiv im Netz betrieben werden müssen.¹²

Die im Alltag gängigste Anordnung ist die Stern-Topologie. Viele Heimnetzwerke als auch Büros setzen auf einen zentralen Knotenpunkt, welcher meist durch den Netzwerkrouter oder Switch realisiert wird. Die Daten werden auf direktem Weg vom Sender, über die Vermittlungsstelle (Router bzw. Switch) zum Empfänger weitergeleitet. In diesem Netzwerk können mehrere Geräte gleichzeitig übergreifend kommunizieren. Weiters werden die Datenpakete nur an den jeweils richtigen Empfänger zugestellt, was die Datenübertragungsgeschwindigkeit im Netzwerk erhöht. Auch hier müssen nicht alle Endgeräte aktiv sein, wohl aber die zentrale Vermittlungsstelle.¹³

Die Topologien Vermascht und Vollvermascht beruhen auf dem Prinzip der Stern-Topologie, jedoch mit der Erweiterung, dass Verbindungswege redundant ausgeführt werden. Dies hat einerseits den Vorteil, dass bei einem Ausfall ein alternativer Transferweg verwendet werden kann. Weiterhin können bei größeren Datenmengen die Datenpakete auf mehreren Wegen zum Ziel gelangen, was zu einer größeren Bandbreite innerhalb des Netzwerkes führt. Im Vollvermaschten Netzwerk ist sogar eine mehrfache Redundanz erkennbar. Die mehrfachen Verbindungswege müssen jedoch budgetär beachtet werden.

Im Bereich der Kleinstbetriebe ist eine einfache Stern-Topologie vollkommen ausreichend. Sie gewährleistet bei geringen Investitionskosten eine gute Verfügbarkeit.

¹¹ Noor N. A. J. E. E. B. Qaqos, „Opnet Based Performance Analysis and Comparison Among Different Physical Network Topologies“, *Academic Journal of Nawroz University (AJNU)*, 1. Januar 2018, 48–54, <https://doi.org/10.25007/ajnu.v7n3a199>.

¹² Qaqos.

¹³ Qaqos.

2.2.2 Netzwerkkomponenten

Um eine entsprechende Topologie realisieren zu können, ist der Einsatz spezieller Netzwerkkomponenten erforderlich. Abbildung 3 zeigt eine schematische Darstellung eines einfachen Unternehmensnetzwerks:

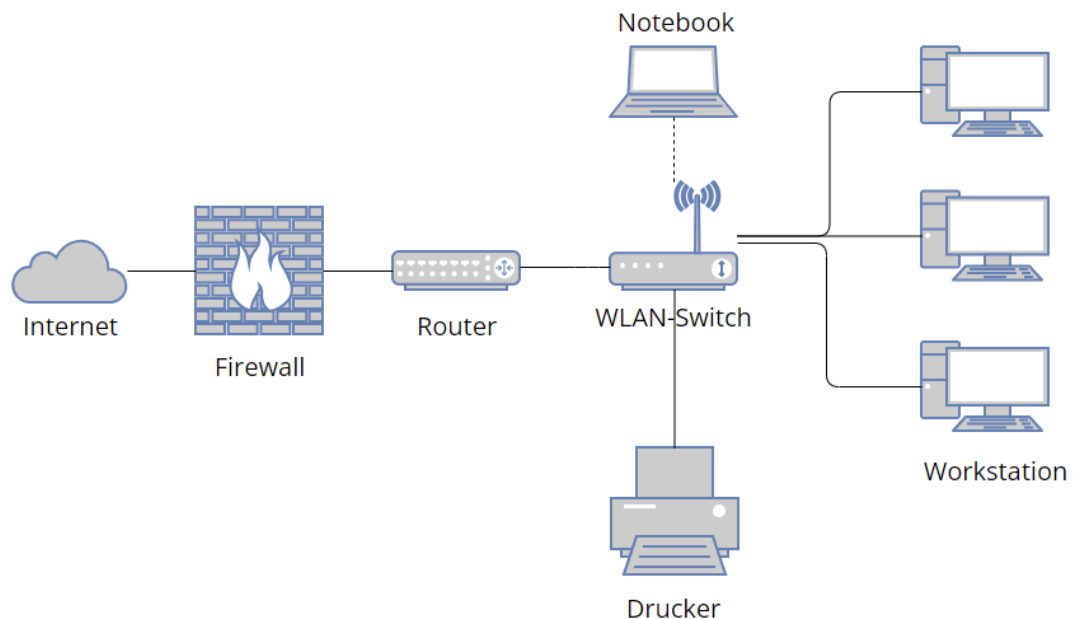


Abbildung 3: Schematische Darstellung eines einfachen Firmennetzwerkes

In den meisten Fällen stellt der Internet-Service-Provider (ISP) ein geeignetes Modem bzw. Router zur Verfügung, um eine Verbindung zu Internet herstellen zu können. Meist ist dieses auch mit einer Firewall ausgestattet. Über den WLAN-Accesspoint bzw. einen Hardware-Switch müssen die einzelnen Clients sowie ein eventueller Server nach der Stern-Topologie verbunden werden, um ein funktionsfähiges Netzwerk herstellen zu können. Folgende Komponenten werden benötigt:

Der Router ist eine Vermittlungseinheit und vermittelt Datenpakete zwischen zwei Computernetzwerken. In unserem Fall ist der Router der Vermittler zwischen dem Internet, das heißt dem Netzwerk des ISP, und unserem Firmennetzwerk.

Die Firewall ist ein Schutzsystem, welches das Firmennetzwerk vor unerlaubten Netzwerkzugriffen schützt.

Der Switch ist die Vermittlungszentrale innerhalb des eigenen Firmennetzwerkes. An ihm werden alle Endgeräte per Netzkabel verbunden, um eine Verbindung herstellen zu können.

Netzwerkkabel bzw. Ethernet-Kabel vom Typ RJ45 werden benötigt, um die Netzwerkkomponenten miteinander zu verbinden (Siehe Abbildung 4). Derzeitiger Standard sind Kategorie 7 (CAT 7) Netzwerkkabel, welche aufgrund ihrer Abschirmung und der verwendeten Übertragungsfrequenz eine Übertragungsrate von bis zu 10 Gigabit pro Sekunde zulässt.



Abbildung 4: Netzwerkkabel

Netzwerkkarten sind geräteseitig bei allen Endgeräten für die Verbindung zwischen Gerät und Netzwerkkabel und in weiterer Folge Switch notwendig, um eine Verbindung mit dem Firmennetzwerk aufbauen zu können. Mobile Geräte können ebenfalls mit einer WLAN-Verbindung und über einen WLAN-Accesspoint kabellos auf das Netzwerk zugreifen.

2.2.3 Server in Kleinstbetrieben

Es ist abzuwägen, wie in einer Firma Dateien und Dienste miteinander geteilt und verwendet werden. Dahingehend richtet sich auch die Planung nach einem möglichen Server. Im einfachsten Fall wird eventuell gar kein Server notwendig sein, wenn im Unternehmen lediglich der Datenaustausch bzw. ein zentraler Datensicherungsort benötigt wird. Dies kann über gängige Router per USB-Festplatte bzw. durch einen einfachen NAS-Datenspeicherort realisiert werden. Auch hier ist es möglich, im System des Routers bzw. des Netzwerkspeichers Benutzer zu hinterlegen und diese bestimmte Rechte auf die Pfade des Netzwerkspeicherortes freizugeben. Auch der gemeinsame Druckerzugriff ist ohne echten Server möglich.

Sollten mehr Dienste oder Funktionen benötigt werden, wird ein NAS mit Verwaltungsmöglichkeiten bzw. ein echter Server benötigt. Beide Möglichkeiten bieten dem Administrator die Handhabung Rechte und Einschränkungen zu konfigurieren. Sollten Datenbanken, Fernzugriffe und VPN-Verbindungen für den Geschäftsbetrieb notwendig sein, ist eine Server-Lösung unumgänglich.

Der Server als zentraler Datenspeicherort sowie als zentraler Datenbank-Host ermöglicht dem Administrator am Standort eine einfache Verwaltung. Je nach Unternehmensgröße und Entwicklung kann der Server eine schnelle Anpassung an die Erfordernisse einer Firma gewährleisten. Auch bei einer Expansion (mehreren Standorten, mehr Mitarbeiterinnen und Mitarbeiter) können zentral schnell die passenden Konfigurationen angepasst und verteilt werden. In der ersten Zeit ist hier wahrscheinlich auch keine Ressourcen-Aufrüstung (mehr Rechenleistung, Speicherplatz, ...) notwendig. Lizenzen sind jedoch anzukaufen. Details zu diesen Zugriffslizenzen sind in Abschnitt 2.2.4 erläutert.

2.2.4 Lizenzierung

Je nachdem welche Konfiguration letztendlich verwendet wird, ist es notwendig die benötigten Dienste und Systeme ordnungsgemäß zu Lizenzieren. In Falle einfacher NAS-Lösungen ist eine Lizenzierung nicht notwendig bzw. ist eine Lizenz durch den Erwerb des NAS-Speichers meist vorhanden. Sollte ein Windows-Server-Betriebssystem verwendet werden, so ist auf die korrekte Lizenzierung zu achten. Microsoft bietet hier je nach Unternehmensgröße und Funktionsumfang unterschiedliche Lizenzmodelle an. **Tabelle 1: Vergleich Edition/Lizenz Microsoft Windows Server 2022**

zeigt die Lizenztypen und Anwendungsbereiche von Microsoft Server Systemen.

Edition	Ideal für...	Virtualisierungsrechte	Zugriffslizenzen	CPU-Limit
Essentials	Kleine Unternehmen mit Basisanforderungen an die IT; sehr kleine oder keine eigene IT-Abteilung	Installation 1x physikalisch oder 1x virtuell *	keine CALs erforderlich (Limitierung auf 25 User / 50 Geräte)	max. 1 CPU max. 10 Kerne
Standard	Für alle Unternehmen, die erweiterte Features benötigen und im geringeren Umfang virtualisieren	2 virtuelle Windows Server Maschinen **	CALs erforderlich ***	unlimitierte Kerne
Datacenter	Für alle Unternehmen mit hohen Anforderungen an die IT Workloads mit großer Anzahl von virtuellen Systemen	Unlimitiert viele virtuelle Windows Server Maschinen		
Datacenter Azure Edition	Spezielle Lizenz zum Betrieb einer virtuellen Maschine (VM) auf Azure IaaS oder auf einem Azure Stack HCI Cluster	Befindet sich noch in der Public-Preview-Phase.		

Tabelle 1: Vergleich Edition/Lizenz Microsoft Windows Server 2022¹⁴

Je nach Mitarbeiter- bzw. Clientanzahl sowie Rechenleistung muss die Lizenz für die entsprechende Edition angekauft werden. Im Falle eines Kleinstbetriebs mit bis zu 10 Mitarbeitern ist die Essentials-Edition mehr als ausreichend und lässt mögliche Erweiterungen offen.

¹⁴ „Windows Server 2022 Editionsunterschiede – Thomas-Krenn-Wiki“, zugegriffen 2. Januar 2025, https://www.thomas-krenn.com/de/wiki/Windows_Server_2022_Editionsunterschiede.

2.2.5 Datenschutz, Netzwerk- & Datensicherheit

Aufgrund der zunehmenden Digitalisierung werden Daten meist digital verarbeitet und abgelegt. Innerhalb eines Servernetzwerkes werden diese zentral an einem Netzwerkspeicherort gespeichert. Da es sich bei den Daten auch um das Kapital des Unternehmens handelt, sind Datenschutz und Datensicherheit ein zentrales Thema jedes Unternehmens.

Jedes Unternehmen muss bei der Verarbeitung von Daten den Schutz der Daten gewährleisten und entsprechende Maßnahmen treffen. Gesetzlich geregelt sind diese Maßnahmen sowie der Umfang der Datenerhebung und die Speicherdauer in der Datenschutzgrundverordnung (kurz: DSGVO). In dieser werden die Rechte und Pflichten des Datenverarbeiters, also auch die Rechte der betroffenen Personen eindeutig geregelt.¹⁵

Die Datensicherheit gewährleistet, dass unbefugte bzw. fremde Benutzerinnen und Benutzer keinen Zugriff auf die in der Firma gespeicherten Daten hat. Hierzu werden Benutzer-Accounts mit personalisierten Passwörtern angelegt. Jeder Mitarbeiter erhält über seine persönlichen Zugangsdaten Zugriff auf das Firmennetzwerk. Wenn mehrere Benutzer im selben Aufgabenbereich arbeiten, könne Sie auch zu einer Gruppe bzw. Sicherheitsgruppe zusammengefasst werden. Aufgrund der einzelnen Zugänge ist es für den Domain- und Netzwerkadministrator nachvollziehbar, wer und wann Daten verändert, gelöscht oder erstellt wurden. Auch können durch entsprechende Sicherheitsrichtlinien Benutzer bzw. Gruppen Schreib-, Lese und weitere Rechte anhand des Role Based Access Control (RBAC)-Modells vergeben werden.

Weiters muss die Datensicherheit eine Datenintegrität sowie Datenauthentizität aufweisen. Es muss daher gewährleistet sein, dass die Daten stets authentisch und frei von unerlaubten Änderungen (Manipulationen) bzw. Fehlern sind und aus sicheren Quellen stammen.

Um einen effektiven Datenschutz gewährleisten zu können müssen regelmäßige Sicherungskopien (Backups) des Datenstands angefertigt werden. Diese sollten in regelmäßigen Abständen, auf ein externes Speichermedium bzw. an einen externen Speicherort transferiert werden und ebenfalls vor dem Zugriff ungebeugter verwahrt und gesichert werden.

Die Netzwerksicherheit muss sicherstellen, dass unerlaubte Benutzerinnen und Benutzer keinen Zugriff auf das physische und auch virtuelle Netzwerk haben. Hierbei muss unter anderen gewährleistet werden, dass sich nicht per einfachen Anschluss an eine

¹⁵ Regina Becker u. a., „Applying GDPR roles and responsibilities to scientific data sharing“, *International Data Privacy Law* 12, Nr. 3 (1. August 2022): 207–19, <https://doi.org/10.1093/idpl/ipac011>.

freie Netzwerkdose Zugriff auf das Firmennetzwerk verschaffen können. Somit sind Zugangspunkte zu sichern bzw. abgekoppelt zu lassen bzw. auch der Datenverkehr selbst über die Netzwerkleitungen zu verschlüsselt (u.a. mit IPsec). Funkverbindungen z.B. über WLAN sind mit einem entsprechend sicheren Verschlüsselungsstandard und komplexen Passwort abzusichern.¹⁶

2.3 Webgehostete Services

Die zunehmende Digitalisierung neben dem Ausbau der Internet- und Netzwerkinfrastruktur treibt den Einsatz webgehosteter Services voran. Viele Unternehmen nutzen diese Dienste für eine anpassungsfähige, einfach skalierbare und/oder kostengünstige IT-Landschaft innerhalb des Unternehmens. Der Abschnitt zeigt die Eigenschaften Anwendungsfelder sowie deren Einfluss auf die Organisation von Unternehmen.

2.3.1 Entwicklung und Verbreitung webgehosteter Services

Schon in den späten 1990-Jahren wurde von der Firma Salesforce, Inc. die erste komplett webbasierende Software-Plattform veröffentlicht.¹⁷ Sie richtete sich primär an Geschäftskunden zur Verwaltung der Mitarbeiterinnen und Mitarbeiter, Dateimanagement, Reporting und Workflows. Damals noch unter der Bezeichnung *Application Service Provider* (ASP) bot Salesforce seine Kunden eine in sich abgeschlossene Arbeitsumgebung an, wobei die benötigte Infrastruktur vollständig bereitgestellt wurde. Eine eigene Infrastruktur beim Kunden entfiel komplett. Salesforce stellte die Rechenleistung und den Speicherort bereit und gewährleistete zudem Netzwerk- und Datensicherheit.

Durch die wachsende Internetgeschwindigkeit und die stabileren Netzwerke wurden auch andere Firmen auf das Potenzial aufmerksam. U.a. startete Google im Jahr 2006 mit Google Docs eine cloudbasierende Variante des bekannten Microsoft Office Suites, welches dadurch schnell zu einem Konkurrenzprodukt wurde.¹⁸ Nach und nach stieg die Akzeptanz der Unternehmen, Kerngeschäftsprozesse auszulagern. Durch die immer zunehmende Digitalisierung der Arbeitsabläufe und den weiteren Ausbau immer schnellerer Datenübertragungswege für das Internet durch Glasfaser und 5G haben viele bekannte Softwareunternehmen ihre Produktpalette erweitert. Dazu gehören auch die Clouddienste. Einige haben ihre Produkte sogar gänzlich auf diese Bereitstellungsform

¹⁶ Asmaa Halbouni, Lee-Yeng Ong, und Meng-Chew Leow, „Wireless Security Protocols WPA3: A Systematic Literature Review“, *IEEE Access* 11 (1. Januar 2023): 112438–50, <https://doi.org/10.1109/ACCESS.2023.3322931>.

¹⁷ „Salesforce Official Web Site“, Salesforce, zugegriffen 2. Januar 2025, <https://www.salesforce.com/de/company/our-story/>.

¹⁸ „Google Docs | History, Features, & Facts | Britannica“, 13. Dezember 2024, <https://www.britannica.com/topic/Google-Docs>.

umgestellt. Dadurch haben sich auch die Lizenzierungsmodelle und die technische Realisierung geändert.

Heutzutage kann man auf viele webgehostete Services zurückgreifen, die lokale Software und Dienste erweitern bzw. ersetzen. Diese werden jedoch nicht mehr einmalig angekauft und lokal betrieben. Vielmehr werden diese Services meist mit einem Abonnement-Modell als Dienstleistungspaket vermarktet. Sie werden unter den Bezeichnungen Software as a Service (kurz: SaaS), Plattform as a Service (kurz: PaaS) und Infrastructure as a Service (IaaS) angeboten. Dieses Modell kann je nach Unternehmensart und Anforderungsprofil Vor- aber auch Nachteile haben, die Vor- und Nachteile dieser Modelle werden ausführlich in Kapitel 2.4 beschrieben.

2.3.2 Funktionsumfang

Heutzutage bieten fast alle Anbieter und Firmen ihre Software-Produkte als cloudgehostete Alternative an. Der Funktionsumfang der Online-Lösung richtet sich dabei meist nach dem gebuchten Tarifmodell und kann somit nicht pauschal definiert werden. Prinzipiell ist festzuhalten, dass das Grundpaket eine solide Arbeitsumgebung darstellt, mit der in den meisten Fällen gut gearbeitet werden kann. Erweiterungen, sogenannte Add-Ons bzw. das Upgraden in ein höheres Paket/höheren Tarif schaltet weitere Funktionen bzw. Ressourcen der Arbeitsoberfläche frei. In den meisten Fällen sind dies erweiterte Auswertungsmöglichkeiten, verbesserte kollaborative Arbeitsmöglichkeiten, mehr Speicherplatz, mehr Sicherheitsfeatures und eine längere BackUp-Speicherdauer.

Mittlerweile zeigt die Entwicklung, dass es ohne webgehostete Anwendungen nicht mehr geht. In Zeiten von Homeoffice und Remote-Working können oder wollen viele Firmen nicht die benötigte interne Infrastruktur bereitstellen, um ein effizientes Arbeiten zu gewährleisten. Aber auch kleinere Softwareunternehmen und -entwickler können teilweise nicht die bereits zu lokal installierter Software auf eine entsprechende Weblösung umbauen bzw. ist dies mit einer Kostenexplosion verbunden. Hierfür nutzen jedoch viele die Möglichkeit des Hostings auf einem angemieteten Server. Die vorhandene Software wird hier lokal installiert. Der Kunde erhält anschließend einen Remote-Session-Zugriff mit entsprechenden Rechten und kann mittels Remote-Bildschirm seine Tätigkeiten in der gewohnten Arbeitsumgebung durchführen. Die lokale Installation im Büro entfällt. Die Wartung und der Betrieb ist Bestandteil des Tarifmodells der jeweiligen Firma, welche auch die technische Möglichkeit anbietet.¹⁹

¹⁹ Federico Etro, „The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe. An Application of the Endogenous Market Structures Approach to a GPT Innovation“, *Review of Business and Economic Literature* LIV, Nr. 2 (2009): 179–208.

Durch die zunehmende Automatisierung und der Integration künstlicher Intelligenz werden die webbasierten Anwendungen nochmals attraktiver. Eine Datenanalyse, deren Auswertung sowie die darauf resultierenden Ergebnisse können kaum von Servern im eigenen Unternehmen bewerkstelligt werden. Da diese Entwicklung mittlerweile zu einem wichtigen Faktor für das wirtschaftliche Überleben geworden ist, werden viele Firmen dazu gedrängt, webbasierte Dienste dort einzusetzen, wo es möglich ist.²⁰

2.3.3 Technische Voraussetzungen

Um webgehostete Services und Dienste verwenden zu können ist eine stabile Internetverbindung notwendig. Je nach Anzahl der Mitarbeiterinnen und Mitarbeiter, Anzahl Clients im Firmennetzwerk und den Anforderungen des Betriebs müssen unter anderen folgenden Fragen beantwortet werden:

- Arbeiten alle Mitarbeiter zeitgleich u.a. mit demselben Dienst(en)?
- Werden (oft) Videokonferenzen über das Internet geführt?
- Werden (oft) größere Datenmengen über das Internet gesendet, womöglich sogar zeitgleich?
- Werden lokale Backups im Unternehmen der webgehosteten Services angefertigt?
- Werden zukünftig weitere webgehostete Dienste und Anwendungen in Betracht gezogen?

Rückgrat der Nutzung von webgehosteten Dienste und Anwendungen ist das korrekt installierte und betriebene physische Netzwerk am Unternehmensstandort sowie die Internetanbindung. Innerhalb des Betriebs bildet die standardisierte strukturelle Verkabelung mit CAT7 bzw. CAT8 Ethernet-Kabeln mit RJ45 Anschluss eine solide und zukunfts-sichere Verbindung an das Firmennetzwerk mit Geschwindigkeiten von bis zu 10 Gbit/s.²¹ Die Anbindung an das Internet erfolgt nach Rücksprache mit dem ISP über die (eigene) Firewall und dem Router. Hierbei gibt es folgendes zu beachten:

- Der Durchsatz der Hardware-Firewall muss auf die Größe und die Datenübertragungsmengen des Betriebs abgestimmt werden.
- Die gebuchte Bandbreite für Down- & Upload-Geschwindigkeiten beim ISP muss entsprechend der Nutzung und der Unternehmensanforderungen gewählt werden.

²⁰ Nikolaos-Alexandros Perifanis und Fotis Kitsios, „Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review“, *Information* 14, Nr. 2 (Februar 2023): 85, <https://doi.org/10.3390/info14020085>.

²¹ „Ethernet Cables Explained: Choosing The Right RJ45 Standard | Next7 IT“, 22. März 2024, <https://www.next7it.com/insights/ethernet-cables-explained-choosing-the-right-rj45-standard/>.

- Je nach Anforderungen und vorhandenen Gegebenheiten muss die Anbindung an das Internet in Hinblick auf Ausfallsicherheit, Reaktionszeit/Latenz und Stabilität gewählt werden.

Klassisch wird die Anbindung von Firmen derzeit per DSL bzw. Koaxialkabel realisiert. Mit einem Investitionsvolumen von fast 1,5 Mrd. Euro wird seitens des Bundes seit 2020 aktiv in den Ausbau des Glasfasernetzes investiert.²² Dies ermöglicht eine schnelle, verlustfreie und latenzfreie Anbindung der Unternehmen. Nichtsdestotrotz findet dieser Ausbau gerade erst statt und liegt seinem Zeitplan hinterher. Bis zum fertigen Ausbau bzw. auch danach kann/muss überlegt werden, ob eine zweite Internetanbindung über ein anderes Übertragungsmedium (z. B. 5G/LTE) sinnvoll erscheint, um bei einem eventuellen Internetausfall den laufenden Betrieb aufrechtzuerhalten bzw. datentransferspitzen abzufedern.

Bzgl. der benötigten Bandbreiten pro Benutzer in einem Unternehmensnetzwerk findet sich in der Literatur kein pauschaler Wert, da dieser von Anforderungsprofil des Unternehmens abhängig ist. Dennoch kann grob folgendes festgehalten werden:

„Für ein Unternehmen mit 20 Benutzern, von denen die Hälfte E-Mail-Funktionalität nutzt und im Internet surft, sollte eine Up- und Download-Geschwindigkeit von 80 Mbps ausreichen. Die andere Hälfte, die regelmäßig Web-Konferenzen und Desktop-Replizierung benötigt, profitiert ebenfalls von dieser Bandbreite, sofern keine gleichzeitige hohe Datenlast entsteht. Dies gewährleistet eine stabile Verbindung für alle Nutzerbedürfnisse.“²³

Einschneidender Faktor hier sind die Live-Streams der Bild- und Tonübertragungen der Videokonferenzen, welche eine gewisse Bandbreite reservieren und belegen. Datenänderungen in Online-Datenbanken bzw. das Versenden von Dokumenten und Dateien in unregelmäßigen und kurzen Abständen können auch bei noch niedrigeren Bandbreiten durchgeführt werden. Laut der obigen Rechnung benötigt ein Kleinunternehmen mit max. 10 Mitarbeitern daher eine minimale Bandbreite von 40Mbit/s. Empfehlungen sagen, dass bei einem Unternehmen mit bis zu 8-10 Mitarbeiter eine Datenübertragungsraten von mind. 50-75 Mbit/s benötigt wird, um einen reibungslosen Betrieb zu ermöglichen. Diese Rechnung beinhaltet auch die Möglichkeit Backups über das Internet zu erstellen.

²² „Breitbandstrategie 2030“, zugegriffen 2. Januar 2025, https://data.breitbandbuero.gv.at/PUB_Breitbandstrategie-2030.pdf.

²³ „Der richtige InternetZugang für Ihr Unternehmen“, zugegriffen 2. Januar 2025, https://cdn2.hubspot.net/hubfs/344164/2016_DE_3forfree/Interactive_broadband_guide_DE.pdf.

2.3.4 Datenschutz & Datensicherheit

Gemäß der EU-Datenschutzgrundverordnung (DSGVO) haben Anbieter von webgehosteten Services aktiv zum Schutz aller gespeicherten Daten insbesondere vor unbefugten Zugriff, Verlust oder Manipulation, Sorge zu tragen.²⁴ Hierzu ist der jeweilige Dienstleister verpflichtet entsprechende Sicherheitsmechanismen in Form von Verschlüsselung der Dateien beim Abruf oder Transfer, regelmäßige Sicherheitsüberprüfungen sowie klare Richtlinien zur Datenspeicherung und -löschung einzuhalten.

2.4 Vor- und Nachteile von lokalen Serversysteme und webgehosteten Services

Ob lokales Serversystem, oder angemietete webgehostete Infrastruktur, beide Versionen haben ihre jeweiligen Vor- und Nachteile. Im Folgenden Abschnitt werden die wichtigsten Bereiche in den jeweiligen Varianten miteinander verglichen.

2.4.1 Kosten

Bei Erstellung bzw. Neukonfiguration eines Unternehmensnetzwerkes sind hohe Investitionskosten aufgrund von Hardware- & Lizenzankauf sowie die benötigte Arbeitszeit zu berücksichtigen. Weiters sind regelmäßige Wartungskosten sowie der turnusmäßige Austausch der Hardware miteinzukalkulieren. Diese Aufgaben werden meist an ein größeres Team in eigene IT-Abteilung vergeben bzw. ein Klein- und Kleinstunternehmer an externe Firmen vergeben, weshalb hier auch mit entsprechendem Kosten zu rechnen ist. Weiters ist eine entsprechende Vorlaufs- und Umsetzungszeit einzukalkulieren.

Webgehostete Plattformen sind meist vorkonfiguriert und können binnen weniger Minuten eingesetzt werden. Es wird nur eine minimale Infrastruktur am Standort benötigt. Abgerechnet wird meist über ein monatliches bzw. jährliches Abo-Modell, welches pro Nutzer bzw. pro Gerät abrechnet. Wartungskosten und Updates sind im Preis inbegriffen.

Fazit: Es ist abhängig von den Bedürfnissen der Firma, welche Variante vorteilhafter ist. Sollten vermehrt interne Dienste und Datenbanken verwendet werden, ist eine lokale Serverumgebung zu bevorzugen. Durchzurechnen ist jedenfalls jeder Break Point in der

²⁴ Masoud Barati und Omer Rana, „Tracking GDPR Compliance in Cloud-Based Service Delivery“, *IEEE Transactions on Services Computing* 15, Nr. 3 (Mai 2022): 1498–1511, <https://doi.org/10.1109/TSC.2020.2999559>.

Kostenrechnung, wobei die Summe der monatlichen bzw. jährlichen Kosten der webgehosteten Services höher als der Betrieb einer eigenen Infrastruktur samt Dienstleister ist. Ab diesem Punkt sollte eine selbstverwaltete Umgebung angestrebt werden.

2.5 Zugriff & Zuverlässigkeit

Der Zugriff auf Firmendaten innerhalb des Firmennetzwerkes ist durch die bereitgestellte Infrastruktur meist auf sehr hohem und schnellem Niveau, da es kaum Störfaktoren innerhalb des Gebäudes gibt. Außerhalb kann der Zugriff durch z.B. einen VPN-Zugang ähnlich realisiert werden, jedoch ist hier die Internetanbindung ein entsprechender Flaschenhals bei vor allem Netzwerk lastigen Anwendungen (z.B.: Datenbankanwendungen).

Anwendungen, welche in Rechenzentren gehostet werden, sind meist über mehrere redundanten Internetleitungen mit viel höherer Bandbreite verbunden. Der Benutzer verbindet sich direkt über eine beliebige Internetverbindung mit dem Servicebetreiber.

Wartungszeiträume sind bei beiden Varianten möglich und meist auch im selben Ausmaß zu finden.

Fazit: Sollten netzwerklastige Anwendungen auch außerhalb des Unternehmens verwendet werden, dann ist eine Auslagerung anzudenken. Mit steigender Mitarbeiterzahl sind Speicherplatzressourcen anzupassen als auch parallele VPN-Zugriffe mitunter eingeschränkt möglich, da die Internetanbindung des Unternehmens durch beidseitige Nutzung an die Kapazitätsgrenze kommt.

2.5.1 Implementierungszeit & Anpassungsmöglichkeiten

Selbstgehostete Netzwerkumgebungen müssen geplant, beschafft, konfiguriert und getestet werden. Dies benötigt viel Zeit, Knowhow und ist nicht kosten- sondern eben auf zeitintensiv. Vorteile ergeben sich jedoch im Aufbau und an der Struktur. Aufgrund der eigenen Infrastruktur sind Anpassungen und Konfigurationen sehr einfach und zufriedenstellend umsetzbar. Auch Speziallösungen bzw. individualisierte Anpassungen können einfacher realisiert werden. Auf Probleme kann schnell und effizient reagiert werden.

Cloudbasierte Lösungen sind meist sofort einsatzbereit, in sich abgeschlossen und erlauben keinen Zugriff auf das Backend des Dienstleisters durch den Kunden. Der Kunde erhält lediglich im Frontend die entsprechenden Berechtigungen zur Administration der Anwendung. Bei Ressourcenknappheit muss meist ein höheres Abo-Modell bzw. ein höherer Tarif abgeschlossen werden. Bei Programm- bzw. Plattformfehlern ist man vom Supportteam des Dienstleisters abhängig. Bei standardisierten Anwendungen können

mitunter gar keine individuellen Anpassungen getätigt werden bzw. sind diese nur mit hohem finanziellem Aufwand umsetzbar.²⁵

Fazit: Es ist abzuwägen, wie schnell eine Arbeitsumgebung und in welchem Ausmaß verfügbar sein soll. Auch wenn webgehostete Services mitunter sofort einsatzbereit sind, können Grundanwendungen (E-Mail, Office-Programme, File-Transfer, etc.) binnen weniger Tage verlässlich auch lokal eingerichtet und betrieben werden, wenn die entsprechende Hardware vorhanden ist.

2.5.2 Datenschutz & Sicherheit

Selbstgehostete Serverumgebungen erlauben das Speichern von Daten lokal am Firmenstandort mit dem Vorteil, dass das Unternehmen selbst immer Herr über die eigenen Daten ist. Bei entsprechenden zusätzlichen Mitarbeiterschulungen kann davon ausgegangen werden, dass die Daten nur innerhalb des beruflichen Umfeldes gespeichert und ausgewertet werden. Jedoch ist auch die Firma selbst verantwortlich entsprechende Vorkehrungen zur Netzwerksicherheit und zum Datenschutz vorzunehmen, sowie eine geeignete Backup-Strategie zu entwickeln.

Unternehmensdateien auszulagern und beim Dienstleister zu speichern, birgt die Gefahr, nie genau zu wissen, wo die Dateien sind. Es besteht auch die Unsicherheit, wer Zugriff darauf hat und wie diese unter anderem auch vom Dienstleister selbst verarbeitet werden. Weiters ist man bzgl. des Zugriffs dem Anbieter ausgeliefert, sollte er den Zugriff aus welchen Gründen auch immer Sperren. Aufgrund der Datenschutzgrundverordnung der Europäischen Union (DSGVO) sind alle Unternehmen, welche Daten elektronisch Verarbeiten (also auch speichern) zum Abschluss einer Datenverarbeitungsvereinbarung verpflichtet, welche die Gegenseiten Rechte und Pflichten regeln. Hierbei werden Minimalanforderungen durch die EU vorgegeben, welche weltweit einen erhöhten Standard gegenüber anderen Ländern bietet.²⁶ Zu beachten ist somit der Standort des Rechenzentrums des Dienstleisters, da die DSGVO auf die Europäische Union begrenzt gültig ist. Weiters bin ich als Kunde abhängig von der Sicherheitsstrategie des Anbieters und deren eingesetzten Ressourcen.

Fazit: Rein rechtlich sind Daten auch bei webgehosteten Anbietern sicher und geschützt. Dies nachzuvollziehen und zu kontrollieren ist meist schwer bzw. nicht möglich. Blindes Vertrauen ist jedoch auch nicht möglich. Es ist somit wieder abzuwägen, ob man alle

²⁵ N. Pramod, Anil Kumar Muppalla, und K. G. Srinivasa, „Limitations and Challenges in Cloud-Based Applications Development“, in *Software Engineering Frameworks for the Cloud Computing Paradigm*, hg. von Zaigham Mahmood und Saqib Saeed (London: Springer, 2013), 55–75, https://doi.org/10.1007/978-1-4471-5031-2_3.

²⁶ Argyri Pattakou u. a., „A Unified Framework for GDPR Compliance in Cloud Computing“, in *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024: The 19th International Conference on Availability, Reliability and Security, Vienna Austria: ACM, 2024)*, 1–9, <https://doi.org/10.1145/3664476.3670918>.

Unternehmensdaten auslagert, und sensible Daten eigens verwaltet und ob zusätzliche lokale Backups aus der Cloud sinnvoll erscheinen, um einen Verlust vorzubeugen. Auf jeden Fall sollte bedacht werden, dass die Verwendung und Auswertung durch den Dienstleister möglich ist, auch wenn dies vertraglich ausgeschlossen ist. Als Firma muss über die Notwendigkeit dieser Auslagerung nachgedacht werden.

2.5.3 Zusammenfassung / Tabellarische Ansicht

Tabelle 2 soll nochmals kurz die Vor- und Nachteile der lokalen Serverumgebung und webgehosteten Services aufzeigen und vergleichen:

	lokale Serverumgebung	Webgehostete Services (SaaS)
Kosten	Hohe Anfangsinvestitionen für Hardware und Lizenzen Regelmäßige Wartungskosten	Niedrigere Anfangskosten Abo- oder Nutzungsgebühren ohne Anschaffungskosten
Wartung/Betrieb	Wartung und Updates sind vom Unternehmen zu verwalten Eigene IT-Abteilung erforderlich (bzw. externe Firma)	Wartung und Updates werden vom Anbieter übernommen Kein Bedarf an interner Wartung
Zugriff und Mobilität	Zugriff häufig nur innerhalb des Unternehmensnetzwerks möglich Eingeschränkte Mobilität	Zugriff von überall mit Internetverbindung möglich Hohe Flexibilität und Mobilität für Mitarbeiter
Skalierbarkeit	Skalierung erfordert zusätzliche Hardwareinvestitionen Kann zeitaufwendig sein	Skalierbar nach Bedarf durch einfache Anpassungen Anbieter übernimmt die Ressourcenverwaltung
Datenschutz und Kontrolle	Hohe Kontrolle über die Daten und deren Sicherheit Daten bleiben im eigenen Haus	Daten werden extern gespeichert Abhängigkeit von den Sicherheitsmaßnahmen des Anbieters
Sicherheitsrisiken	Risiko für interne Sicherheitsverletzungen Physische Sicherheitsvorkehrungen nötig	Höheres Risiko für externe Cyberangriffe Anbieter haben oft strenge Sicherheitsprotokolle
Anpassungsmöglichkeiten	Hohe Flexibilität bei individuellen Anpassungen und Konfigurationen	Weniger Anpassungsmöglichkeiten, oft standardisiert Anbieterabhängig, welche Anpassungen möglich sind
Implementierungszeit	Lange Implementierungszeit Einrichten und Testen der Hardware erforderlich	Schnelle Implementierung, da kein Hardwareaufbau nötig Sofort einsatzbereit
Zuverlässigkeit	Abhängig von eigener Infrastruktur und IT-Kompetenz	Abhängig von der Zuverlässigkeit des Anbieters Anbieter bieten häufig hohe Verfügbarkeit und Redundanz
Upgrades und Updates	Müssen manuell durchgeführt werden Möglicherweise zusätzliche Kosten	Automatische Updates durch den Anbieter Meist in den Kosten inbegriffen

Tabelle 2: Vergleich der Vor- und Nachteile von lokalen Serverumgebungen und webgehosteten Services

2.6 Aktueller Forschungsstand

In den letzten Jahren hat die Forschung zu webgehosteten Services und deren Einsatz in Kleinunternehmen erheblich zugenommen. Diese Entwicklungen sind insbesondere durch die Digitalisierung und die Auswirkungen der COVID-19-Pandemie beschleunigt worden.²⁷ Der folgende Abschnitt gibt einen Überblick über die aktuellen Trends, Herausforderungen und Erkenntnisse in diesem Bereich.

2.6.1 Digitalisierung und Cloud-Computing

Die Digitalisierung hat die Art und Weise, wie Unternehmen arbeiten, revolutioniert. Laut einer Studie von Gartner (2023) nutzen mittlerweile über 70 % der Unternehmen Cloud-Services, um ihre IT-Infrastruktur zu optimieren.²⁸ Diese Services bieten nicht nur Kosteneinsparungen, sondern auch Flexibilität und Skalierbarkeit, die für Kleinunternehmen von großer Wichtigkeit sind. Die Forschung zeigt, dass Unternehmen, die auf Cloud-Lösungen umsteigen, in der Lage sind, ihre Betriebskosten, um bis zu 30 % zu senken.²⁹

Ein zentraler Aspekt der Digitalisierung ist die Möglichkeit, IT-Ressourcen bedarfsgerecht zu skalieren. Dies ermöglicht es Kleinunternehmen, ihre IT-Kosten zu optimieren und gleichzeitig die notwendige Leistung bereitzustellen, um wettbewerbsfähig zu bleiben. Die Implementierung von Cloud-Services hat auch die Einführung neuer Geschäftsmodelle gefördert, die auf Agilität und Innovation abzielen.

2.6.2 Sicherheitsaspekte

Ein zentraler Themenschwerpunkt in der aktuellen Forschung ist die Sicherheit von webgehosteten Services. Die Datenschutz-Grundverordnung (DSGVO) hat die Anforderungen an den Datenschutz in der EU verschärft, was Unternehmen dazu zwingt, ihre Datenstrategien zu überdenken. Studien zeigen, dass viele Kleinunternehmen Schwierigkeiten haben, die erforderlichen Sicherheitsstandards zu erfüllen.³⁰

Die Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung, Multi-Faktor-Authentifizierung und regelmäßigen Sicherheitsüberprüfungen ist unerlässlich, um das Vertrauen der Kunden zu gewinnen und rechtlichen Anforderungen gerecht zu werden.

²⁷ Sahut und Lissillour, „The Adoption of Remote Work Platforms after the Covid-19 Lockdown“.

²⁸ „Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600bln in 2023“, zugegriffen 2. Januar 2025, <https://www.zawya.com/en/press-release/research-and-studies/gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600bln-in-2023-b3fygmz3>.

²⁹ Noluthando Zamanjomane Mhlono u. a., „Reviewing the Impact of Cloud Computing on Small and Medium Enterprises in Africa“, *International Journal of Science and Research Archive* 11, Nr. 1 (2024): 1444–51, <https://doi.org/10.30574/ijrsra.2024.11.1.0236>.

³⁰ Barati und Rana, „Tracking GDPR Compliance in Cloud-Based Service Delivery“.

Eine Umfrage von PwC 2023 ergab, dass 60 % der Unternehmen Bedenken hinsichtlich der Datensicherheit in der Cloud haben, was die Notwendigkeit unterstreicht, robuste Sicherheitsstrategien zu entwickeln.³¹

2.6.3 Wirtschaftliche Überlegungen

Die wirtschaftlichen Vorteile von webgehosteten Services sind ein weiterer wichtiger Forschungsbereich. Eine Machbarkeitsstudie von KPMG (2023) hat ergeben, dass Unternehmen, die auf Cloud-Lösungen umsteigen, nicht nur Kosten sparen, sondern auch ihre Effizienz steigern können.³² Die Möglichkeit, Ressourcen nach Bedarf zu skalieren, ermöglicht es Kleinstunternehmen, flexibler auf Marktveränderungen zu reagieren.

Des Weiteren zeigen aktuelle Studien, dass Unternehmen, die Cloud-Services nutzen, eine höhere Innovationsrate aufweisen. Dies liegt daran, dass sie schneller auf neue Technologien zugreifen und diese implementieren können, ohne in teure Hardware investieren zu müssen. Die Untersuchung von Forrester 2024 zeigt, dass der Markt für Cloud-Services in den nächsten fünf Jahren um 25 % wachsen wird, was die Relevanz dieser Technologien für Kleinstunternehmen unterstreicht.³³

2.6.4 Herausforderungen bei der Implementierung

Trotz aller Vorteile gibt es auch Herausforderungen bei der Implementierung von webgehosteten Services. Eine Umfrage von PwC 2023 zeigt, dass viele Kleinstunternehmen Bedenken hinsichtlich der Integration neuer Technologien in bestehende Systeme haben.³⁴ Die Notwendigkeit, Mitarbeiter zu schulen bzw. anzulernen und die Akzeptanz neuer Technologien zu fördern, stellt eine zusätzliche Hürde dar, da gewohnte Ablaufprozesse durch neue ersetzt werden.

Ergebnisse deuten darauf hin, dass eine klare Kommunikationsstrategie und Schulungsprogramme ausschlaggebend sind, um die Akzeptanz zu erhöhen und den Übergang zu erleichtern. Unternehmen, die in Schulungen investieren, berichten von einer höheren Mitarbeiterzufriedenheit und einer schnelleren Implementierung neuer Systeme, da es hier eine aktive Unterstützung seitens des Arbeitsgebers/der Firma gibt.

³¹ PricewaterhouseCoopers, „From Threat to Opportunity | PwC's Global Risk Survey 2023“, PwC, zugegriffen 2. Januar 2025, <https://www.pwc.com/gx/en/issues/risk-regulation/global-risk-survey.html>.

³² Adrian Bradley, „The Key Cloud Trends in 2023 – and What They Mean for 2024 - KPMG UK“, KPMG, 29. Oktober 2024, <https://kpmg.com/uk/en/home/insights/2023/12/key-cloud-trends-in-2023.html>.

³³ „Predictions 2024: Cloud Computing“, Forrester, zugegriffen 2. Januar 2025, <https://www.forrester.com/webinar/predictions-2024-cloud-computing/WEB40235>.

³⁴ PricewaterhouseCoopers, „From Threat to Opportunity | PwC's Global Risk Survey 2023“.

2.6.5 Zukunftsausblick

Die Forschung zu webgehosteten Services entwickelt sich ständig weiter. Zukünftige Studien werden sich voraussichtlich auf die Integration von Künstlicher Intelligenz (KI) und Maschine Learning in Cloud-Lösungen konzentrieren. Diese Technologien könnten die Effizienz und Sicherheit von webgehosteten Services weiter verbessern und neue Möglichkeiten für Kleinunternehmen schaffen.

Ein weiterer Trend ist die zunehmende Nutzung von hybriden Cloud-Lösungen, die es Unternehmen ermöglichen, sowohl lokale als auch cloudbasierte Ressourcen zu kombinieren. Laut einer Prognose von Forrester 2024 wird erwartet, dass hybride Cloud-Modelle in den nächsten Jahren an Popularität gewinnen, da sie Flexibilität und Kontrolle bieten³⁵.

³⁵ „Predictions 2024“.

3. Machbarkeitsstudie

Die folgende Machbarkeitsstudie bewertet die Umsetzbarkeit eines Wechsels von lokalen Servern zu webgehosteten Services in Kleinunternehmen. Es wird untersucht ob die technische, wirtschaftliche, organisatorische sowie datenschutzrechtliche Machbarkeit gegeben ist, ein lokales Serversystem auf ein webgehostetes System umzustellen. Die Studie ermittelt die Bedingungen für eine sinnvolle Umstellung und analysiert diese vier Bereiche im Detail auf theoretische Konzepte sowie praktische Herausforderungen und Lösungsansätze. Eine anschließende Zusammenfassung der Ergebnisse bietet eine fundierte Entscheidungshilfe für Kleinunternehmen bei der Überlegung zum Wechsel zu webgehosteten Services.

3.1 Technische Machbarkeit

Die technische Machbarkeit bei der Umstellung von lokalen Servern zu Web-Services benötigt verschiedene Voraussetzungen und muss unter folgenden Gesichtspunkten beurteilt werden: die bestehende IT-Infrastruktur, die Abstimmung mit aktuellen Systemen sowie die Anpassungsmöglichkeiten bzw. Integrationsmöglichkeiten. Im folgenden Abschnitt werden diese Kriterien genauer betrachtet.

3.1.1 Anforderungen an die Infrastruktur

Die Umstellung von lokalen Servern auf webgehostete Services verlangt eine Prüfung der bestehenden IT-Infrastruktur mit Fokus auf Netzwerkkapazität, Latenzzeiten, Geschwindigkeit sowie Sicherheit. Eine schnelle Internetanbindung für den Betrieb ist Voraussetzung dafür, wenn die Daten neben lokaler Anwendungen auch über externe Server verfügbar gemacht werden sollen.

Netzwerkleistung und Bandbreitenanforderungen

Die benötigte Bandbreite richtet sich nach den Anwendungen und der Nutzeranzahl. E-Mail-Dienste oder Cloud-Speicher brauchen wenig Übertragungsleistung. Datenreiche Programme wie Remote-Desktop oder Cloud-ERP benötigen dagegen mehr Kapazität. Eine zu niedrige Upload-Geschwindigkeit erschwert die Nutzung vieler Cloud-Dienste bei der Datensynchronisation und eine zuverlässige Internetverbindung mit schneller Reaktionszeit ist unverzichtbar. In ländlichen Regionen begrenzen langsame DSL-Anschlüsse oft den Wechsel zu Cloud-Lösungen. Firmen mit großem Datenaufkommen benötigen Glasfaser oder spezielle Unternehmensanschlüsse für eine störungsfreie Funktion. Tabelle 3 zeigt die je nach Nutzungsszenario erforderliche Mindestbandbreite und Latenz, weil einem Betreiber mit 10 Mitarbeitern.

Nutzungsszenario	Mindestbandbreite Download	Mindestbandbreite Upload	Anforderungen an Latenz
E-Mail, Web-Browsing, Cloud-Speicher (z. B. OneDrive)	20–50 Mbit/s	5–10 Mbit/s	Unkritisch
Gemeinsame Dokumentenbearbeitung, Videokonferenzen (z. B. Microsoft Teams, Zoom)	50–100 Mbit/s	10–20 Mbit/s	≤ 50 ms
Datenbankanwendungen, Remote-Desktop-Verbindungen	100–200 Mbit/s	20–50 Mbit/s	≤ 30 ms
Unternehmensweite Cloud-ERP-Systeme, Virtualisierung in der Cloud	200+ Mbit/s	50+ Mbit/s	≤ 10 ms

Tabelle 3: Typische Bandbreitenanforderungen nach Nutzungsszenario

Redundanz und Ausfallsicherheit

Ein zentrales Merkmal für webgehostete Dienste ist der Erhalt der Funktion bei Netzausfällen. Lokale Server in einem internen Netzwerk bleiben auch ohne Internet aktiv. Eine unterbrochene Internetverbindung stoppt bei cloudbasierten Systemen jedoch oft den kompletten Betrieb. Unternehmen nutzen deshalb Redundanzlösungen mit alternativen Verbindungen für Ausfälle. Eine zweite Internetleitung eines anderen Anbieters schaltet sich bei Störungen automatisch ein. Mobilfunkbasierte Notfallverbindungen über 5G oder LTE dienen als temporäre Lösung für Internetausfälle. Edge-Caching sowie die lokale Synchronisierung von Cloud-Diensten speichern wichtige Daten vor Ort und können nach Wiederherstellung die Daten neu synchronisieren und andererseits auch als eine Mini-Backup dienen. Das reduziert die Abhängigkeit von einer einzelnen dauerhaften Netzwerkverbindung. Die Firmen müssen aber die Kosten dieser Lösungen prüfen. Die Ausgaben für Redundanz schmälern oft die Vorteile der webgehosteten Services.

Sicherheitsanforderungen und Netzwerkinfrastruktur

Der Wechsel zu webgehosteten Services erfordert neue Ansätze für die Netzwerksicherheit. Lokale Server laufen in abgeschirmter Infrastruktur – Cloud-Dienste haben dagegen

ständigen Internet-Zugang, was zusätzliche Risiken schafft. Bestimmte Sicherheitsmaßnahmen schützen die Integrität oder Vertraulichkeit der Daten. Die Verschlüsselung der Datenübertragung steht im Fokus, wobei TLS/SSL-Protokolle die Kommunikation zwischen Client sowie Cloud-Dienst absichern und unbefugtes Abfangen verhindern. Ein ausgereiftes Identitäts- und Zugriffsmanagement (IAM) steuert Benutzerrechte zentral und bietet durch Multi-Faktor-Authentifizierung (MFA) mehr Schutz. Das interne Netzwerk benötigt Firewall- und Intrusion-Detection-Systeme (IDS) zum Schutz vor unerlaubtem Cloud-Zugriff. Regelmäßige Sicherungskopien neben Notfallplänen ergänzen Cloud-Dienste durch lokale Backups und schützen vor Datenverlusten durch Angriffe oder Systemausfälle. Abzuwägen ist hier jedoch auch, um welchen Typ von Daten es sich handelt. Je nach Branche und Größe sowie Wirtschaftlichkeit muss abgewogen werden, wie hoch das Schutzlevel aufgebaut werden kann. Cloud-Dienste von Unternehmen aus dem Gesundheitswesen oder Finanzsektor müssen höhere Sicherheitsvorkehrungen beachten. Zudem sind branchenspezifischen Sicherheits- und Compliance-Standards einhalten³⁶.

Hardware-Anforderungen für die Nutzung webgehosteter Services

Cloud-Lösungen lagern viele IT-Funktionen aus, doch Endgeräte benötigen weiterhin genug Leistung für moderne Webanwendungen. Eine passende Prozessorleistung ist nötig, weil viele Programme im Browser laufen und lokale Berechnungen durchgeführt werden. Die Endgeräte braucht deshalb eine aktuelle Hardwarekomponenten (Quad-Core Prozessor, 16GB-RAM Arbeitsspeicher, SSD-Festplatte, ...). Gute Netzwerkkarten sowie moderne WLAN-Module sorgen für eine stabile Netzwerkverbindungen. Die Geräte sollten Gigabit-Ethernet oder Wi-Fi 6 (802.11ax) haben, um schnell mit dem Netz zu kommunizieren. Eine neue Investitionskosten entstehen, wenn die vorhandene Hardware diese Bedingungen nicht erfüllt.

3.1.2 Integration bestehender Systeme

Die Einbindung vorhandener IT-Systeme bzw. des Datenbestands in eine Webgehostete Infrastruktur ist eine der Kernpunkte bei der Umstellung. Viele neue Programme sind zwar für Online-Dienste angepasst, doch oft nutzen Firmen noch örtliche Software oder Abläufe, die sich schwer übertragen lassen. Die Anpassung braucht passende Schritte bei der Datenübertragung, der Software-Abstimmung sowie den Zugangskontrollen³⁷.

³⁶ Clement Arhinful und Richard Essah, „Investigating Cloud Computing Security Measures and Risks“, *International Journal of Research Publication and Reviews*, Nr. 5 (Februar 2024): 1642–46.

³⁷ Mohsen Attaran und Jeremy Woods, „Cloud computing technology: improving small business performance using the Internet“, *Journal of Small Business & Entrepreneurship* 31, Nr. 6 (2. November 2019): 495–519, <https://doi.org/10.1080/08276331.2018.1466850>.

Ein zentraler Gesichtspunkt der Systemintegration ist der Transfer bestehender Daten in die Cloud. Lokale Server enthalten oft verschiedene Datenformate, die für Cloud-Dienste angepasst werden müssen bzw. auf eine neuere Formatversion angepasst werden muss. Der Wechsel zu einer cloudbasierten Datenbanklösung erweist sich bei relationalen Datenbanksystemen als anspruchsvoll. Es kann möglich sein, dass der jeweilige Anbieter eine Cloud-Datenbank mit anderen Abfragesprachen oder Strukturen nutzt. Somit müssen die Daten aufbereitet werden. Der Transfer läuft in drei Phasen ab: Datenextraktion, Transformation sowie Import. Dateispeicher wie Dokumente oder Bilder lassen sich einfach übertragen. Aber Anwendungen mit vernetzten Datenstrukturen benötigen eine genaue Prüfung der Relationen und Abhängigkeiten. Eine Hauptaufgabe liegt in der Abstimmung laufender Prozesse beim Transfer, um Ausfälle gering zu halten. Firmen mit dauerhaft aktiven Systemen wie Buchhaltungssoftware oder CRM-Lösungen brauchen Parallelbetriebslösungen. Die Daten bleiben in einer Übergangszeit lokal sowie in der Cloud synchron, bis der finale Wechsel stattfindet. Die Datenkonsistenz steht im Fokus, da gleichzeitige Änderungen in beiden Systemen zu Fehlern führen.

Wenn es der Betrieb zulässt, ist natürlich ein Komplettransfer nach vorheriger Testphase zu empfehlen. Zeitlich eignen sich hierfür Betriebsurlaube bzw. verlängerte Wochenenden. Tabelle 4 zeigt, welche Herausforderungen beachtet werden müssen, sowie eine mögliche, empfohlene Lösung.

Daten Art	Herausforderung bei Migration	Empfohlene Lösung
Strukturierte Daten (SQL-Datenbanken)	Unterschiedliche Datenbanksysteme, Anpassung von Tabellenstrukturen notwendig	Nutzung von Migrations-tools, Vorab-Tests mit Pilotdaten
Unstrukturierte Daten (Dokumente, Bilder, Videos)	Dateiformate und Zugriffsgeschwindigkeiten variieren je nach Cloud-Speicherlösung	Cloud-Speicher mit lokaler Caching-Option wählen
Laufende Transaktionsdaten (z. B. Buchhaltung, ERP)	Migration während des Betriebs kann zu Datenverlusten führen	Temporäre Synchronisation zwischen lokalem Server und Cloud
Benutzerdaten & Zugriffsrechte	Authentifizierungsprotokolle und Benutzerrechte müssen angepasst werden	Einführung von Single Sign On (SSO) oder hybriden Authentifizierungslösungen

Tabelle 4: Herausforderungen und empfohlene Lösungen bei der Migration verschiedener Datenarten

Eine mangelhafte Planung der Datenmigration führt oft zu Datenverlust, Zugriffskonflikten oder Leistungseinbußen. Unternehmen müssen deshalb vorab Testläufe mit bestimmten Daten ausführen, um Fehler rechtzeitig zu erkennen sowie den Umstieg zu verbessern.

Neben der Datenmigration ist die Kompatibilität vorhandener Software eine weitere Herausforderung. Viele aktuelle Anwendungen existieren bereits als Software-as-a-Service (SaaS), doch manche Programme funktionieren nur auf lokalen Servern oder Windows-Server-Umgebungen. Diese Anwendungen lassen sich nicht einfach in die Cloud verschieben. Sie müssen virtualisiert, durch andere Lösungen ersetzt oder umgebaut werden. Die Migration einer Software in die Cloud basiert auf den technischen Vorgaben sowie den Lizenzmodellen der Anwendung und des Herstellers. Manchmal benötigt man eine Hybridlösung, bei der einige Programme lokal bleiben oder mit Cloud-Diensten verbunden werden³⁸.

Softwaretyp	Herausforderung bei der Cloud-Migration	Mögliche Lösungsstrategie
Ältere Windows-Server-Anwendungen	Keine direkte Unterstützung für Cloud-Plattformen	Virtualisierung über Remote Desktop Services oder Windows Virtual Desktop
Branchen- oder Spezialsoftware	Anbieter bietet keine Cloud-Version an	Umstieg auf Cloud fähige Alternativen oder Hybridbetrieb mit lokalem Hosting
Selbstentwickelte Unternehmenssoftware	Abhängigkeiten zu lokalen Datenbanken oder APIs	Anpassung des Codes oder Nutzung von Middleware zur Cloud-Integration
Lizenzierte Software mit hardwaregebundener Aktivierung	Lizenzmodell verhindert Nutzung in virtualisierten Umgebungen	Umstellung auf abonnementbasierte Cloud-Lizenzen oder Nutzung von Lizenzservern

Tabelle 5: Typische Kompatibilitätsprobleme und Lösungsansätze

³⁸ Mahdi Fahmideh u. a., „Challenges in migrating legacy software systems to the cloud an empirical study“ (arXiv, 17. April 2020), <https://doi.org/10.48550/arXiv.2004.10724>.

Eine wichtige Aufgabe bei der Migration zu webgehosteten Services ist die Kontrolle von Benutzerkonten, Rechten und Anmeldeverfahren. Lokale Server basieren oft auf Active Directory (AD) für die Benutzerverwaltung. Cloud-Dienste setzen stattdessen auf OAuth, OpenID Connect oder SSO. Ein Wechsel zum Cloud-Authentifizierungsmodell macht neue Strukturen nötig. Firmen müssen zwischen zwei Optionen wählen: eine hybride Lösung mit lokaler sowie Cloud-Verwaltung oder der komplette Umstieg auf Cloud IAM. Bei hybriden Modellen stellt die Abstimmung der Benutzerrechte eine Hürde dar. Änderungen an lokalen Konten lassen sich nicht selbstständig in Cloud-Systeme übertragen, ohne passende Verbindung zwischen den Systemen. Eine verlässliche Verwaltung benötigt meist zusätzliche Identitätsbrücken oder Cloud-Verzeichnisdienste³⁹.

Merkmal	Lokale Authentifizierung (Active Directory, LDAP)	Cloud-basierte Authentifizierung (SSO, OAuth, IAM)
Verwaltung	Lokale IT-Abteilung verwaltet Benutzerkonten und Berechtigungen	Zentralisierte Cloud-Plattform übernimmt Benutzerverwaltung
Sicherheit	Physische Zugangskontrolle zum Serverraum erforderlich	MFA für besseren Schutz
Skalierbarkeit	Manuelle Verwaltung für neue Nutzer erforderlich	Automatische Benutzerbereitstellung über Cloud-APIs
Integration	Funktioniert nur mit internen Netzwerken	Unterstützung für Web- und mobile Anwendungen
Datenhoheit	Unternehmen kontrolliert alle Benutzerdaten	Abhängig von externem Betreiber

Tabelle 6: Vergleich lokaler und Cloud-basierter Authentifizierungssysteme

3.1.3 Skalierbarkeit & Flexibilität

Die Wahl zwischen webgehosteten Services und lokalen Servern basiert auf der Anpassbarkeit der Lösung. Lokale Server haben feste Grenzen während Cloud-Systeme

³⁹ I. Indu, P. M. Rubesh Anand, und Vidhyacharan Bhaskar, „Identity and access management in cloud environment: Mechanisms and challenges“, *Engineering Science and Technology, an International Journal* 21, Nr. 4 (1. August 2018): 574–88, <https://doi.org/10.1016/j.jestch.2018.05.010>.

flexible Ressourcen bereitstellen. Diese Anpassungsfähigkeit betrifft die technische Basis sowie die betrieblichen oder finanziellen Abläufe.

Die Skalierbarkeit von Web-Services an höhere Bedürfnisse lässt Firmen ihre IT-Kapazitäten flexibel erweitern, ohne große Hardwarekosten. Lokale Server haben fixe Grenzen und brauchen bei steigendem Bedarf neue Hardware. Cloud-Dienste passen Speicher, Leistung oder Bandbreite direkt an den Bedarf an. Ein solcher Aufbau nützt vor allem Firmen mit jahreszeitlichen Schwankungen oder plötzlichem Wachstum, weil sie Ressourcen schnell anpassen können. Die Ausbaufähigkeit hängt jedoch von der Software-Struktur ab. Cloud-optimierte Programme nutzen diese Vorteile besser als große lokale Programme, die sich oft nicht aufteilen lassen⁴⁰. Tabelle 7 zeigt eine Gegenüberstellung der Skalierbarkeit beider Lösungen

Aspekt	Lokale Server	Webgehostete Services
Kapazitätsanpassung	Manuelle Hardwareaufrüstung erforderlich	Automatische Skalierung je nach Bedarf
Investitionskosten	Hohe Einmalkosten für neue Serverhardware	Variable Kosten je nach Nutzung
Performanceoptimierung	Begrenzte Anpassungsmöglichkeiten	Ressourcen flexibel zuweisbar
Wartungsaufwand	Regelmäßige physische Updates notwendig	Anbieter übernimmt Infrastrukturmanagement
Reaktionszeit auf neue Anforderungen	Verzögerungen durch Beschaffungszeiten	Sofortige Anpassung an veränderte Bedingungen

Tabelle 7: Vergleich der Skalierbarkeit und Wartung zwischen lokalen Servern und webgehosteten

Flexibilität bestimmt bei Kleinstunternehmen die Wahl zwischen lokalen Servern oder webgehosteten Diensten. Lokale Server geben mehr Kontrolle über die IT-Struktur, während Cloud-Dienste den Zugriff von überall ermöglichen. Dies nützt besonders Firmen mit Homeoffice oder mehreren Standorten. Die Cloud-Modelle bieten passende Optionen an: Public-Cloud macht Firmen beweglich sowie skalierbar, während Private-Cloud mehr Macht über Datenschutz gibt. Hybridmodelle nutzen beide Vorteile – wichtige Programme bleiben lokal, während andere Abläufe in die Cloud gehen. Der Einsatz von

⁴⁰ Grunnar Brataas u. a., „Scalability Analysis of Cloud Software Services“, in *2017 IEEE International Conference on Autonomic Computing (ICAC)*, 2017, 285–92, <https://doi.org/10.1109/ICAC.2017.34>.

Web-Diensten schafft aber oft Abhängigkeit von Anbietern, da die genutzten Technologien oder APIs einen Plattformwechsel erschweren.

Die wirtschaftliche Tragfähigkeit von webgehosteten Services ist abhängig von den Skalierungskosten über die Zeit. Der erste Einstieg in Cloud-Dienste kostet oft weniger als ein lokaler Server, doch die laufenden Gebühren steigen bei hoher Nutzung. Unternehmen sollten deshalb berechnen, ob sich die Skalierungskosten auf Dauer rechnen⁴¹. Tabelle 8 zeigt eine grobe Analyse der Kosten beider Lösungen

Zeitraum	Lokale Server (Investitionsmodell)	Webgehostete Services (Pay-as-you-go)
Jahr 1	Hohe Anfangsinvestition	Niedrige Grundkosten
Jahr 2–3	Moderate Wartungskosten	Steigende Gebühren bei höherer Nutzung
Jahr 4–5	Notwendige Hardware-Upgrades	Kontinuierliche monatliche Zahlungen
Jahr 6+	Ersatz oder vollständige Erneuerung	Potenziell höhere Gesamtkosten

Tabelle 8: Vergleich der langfristigen Kosten zwischen lokalen Servern und webgehosteten Services

Die wirtschaftliche Entscheidung basiert auf der aktuellen Unternehmensgröße sowie den Plänen für die Zukunft. Für Unternehmen mit wechselndem IT-Bedarf bieten webgehostete Services deutliche Vorteile, da sie ohne dauerhafte Hardwarebindung auskommen. Betriebe mit konstanten Anforderungen nutzen besser eine lokale Serverlösung, da sie nach Abzahlung der Investitionskosten keine weiteren Gebühren entrichten müssen. Trotzdem müssen Komponenten von Zeit zu Zeit ersetzt werden.

⁴¹ Mihail Gaiuanu, „On Premise Data Center vs CLOUD“, in *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2023, 1068–71, <https://doi.org/10.1109/CSCI62032.2023.00176>.

3.2 Wirtschaftliche Machbarkeit

Die wirtschaftliche Machbarkeit einer Umstellung von lokalen Servern auf webgehostete Services bestimmt den Erfolg von Kleinstunternehmen. Eine gründliche Analyse der Wirtschaftlichkeit umfasst drei zentrale Bereiche: den direkten Kostenvergleich beider Lösungen, die Betrachtung von Investitions- und Betriebskosten sowie die Bestimmung des Returns on Investment (ROI).

3.2.1 Kostenanalyse & Vergleich

Die wirtschaftliche Entscheidung zwischen lokalen Servern und webgehosteten Services basiert auf der Kostenstruktur. Lokale Server erfordern eine hohe Anfangsinvestition, während Cloud-Dienste ein Abonnementmodell mit regelmäßigen Zahlungen nutzen. Die unterschiedliche Verteilung der Kosten wirkt sich auf die Liquidität eines Unternehmens sowie auf die langfristige Planung aus. Unternehmen mit ausreichendem Budget ziehen Vorteile aus der direkten Amortisation eines lokalen Servers. Das Cloud-Modell bietet eine einfache Skalierung ohne große Vorabkosten. Die Entscheidung für eine Option richtet sich nach der Finanzlage und den geschäftlichen Bedürfnissen⁴².

Die laufenden Betriebskosten sind neben den Anschaffungskosten ein wichtiger Aspekt der Wirtschaftlichkeit. Lokale Server führen zu stetigen Ausgaben für Wartung, Strom und Updates. Cloud-Anbieter rechnen diese Leistungen in ihre Abonnementgebühren ein. Die Kosten eines lokalen Servers bleiben über lange Zeit konstant, doch Firmen müssen Geld für ungeplante Reparaturen oder neue Hardware zurücklegen. Cloud-Dienste zeigen dagegen eine klare Kostenaufstellung mit festen Monatsbeträgen. Diese Beträge wachsen jedoch schnell bei höherem Verbrauch⁴³.

Ein weiterer Hauptaspekt der Kostenanalyse betrifft die Skalierung der IT-Infrastruktur. Lokale Server sind meist für eine lange Nutzungsdauer konzipiert und lassen sich nur durch neue Hardware erweitern. Cloud-Dienste bieten dagegen eine sofortige Anpassung der Ressourcen nach Bedarf. Diese Flexibilität stellt einen Vorteil für Unternehmen mit wechselnden IT-Bedürfnissen dar, da sie ihre Kapazitäten schnell ändern können. Cloud-Dienste bergen jedoch auf Dauer das Risiko höherer Gebühren, besonders wenn der Anbieter die Preise ändert oder mehr Speicher oder Rechenleistung erforderlich wird. Eine Kostenanalyse umfasst deshalb neben den aktuellen Ausgaben auch eine strategische Bewertung der künftigen Kosten sowie der Anpassungsfähigkeit der IT-Infrastruktur.

⁴² Gaiuanu.

⁴³ Alan Chalker u. a., „Cloud and on-premises data center usage, expenditures, and approaches to return on investment: A survey of academic research computing organizations“, in *Practice and Experience in Advanced Research Computing 2020: Catch the Wave*, PEARC '20 (New York, NY, USA: Association for Computing Machinery, 2020), 26–33, <https://doi.org/10.1145/3311790.3396642>.

3.2.2 Investition & Betriebskosten

Die finanziellen Bedingungen entscheiden über die wirtschaftliche Sinnhaftigkeit von lokalen Servern oder webgehosteten Services. Ein lokaler Server erfordert zu Beginn eine große Investition für Hardware, Softwarelizenzen, Installation und gegebenenfalls die Hilfe von externen IT-Dienstleistern. Firmen müssen diese Summe vorab aufbringen und über mehrere Jahre abschreiben. Webgehostete Services hingegen benötigen keine hohe Anfangsinvestition, da ein externer Anbieter die IT-Ausstattung zur Verfügung stellt. Die Ausgaben fallen hier als monatliche oder jährliche Gebühren an und richten sich nach dem Verbrauch und den gewählten Paketen. Lokale Server bieten feste Kosten auf lange Sicht, während Cloud-Lösungen schwankende Beträge aufweisen, die mit steigendem Verbrauch steigen können⁴⁴.

Neben den Anschaffungskosten fallen auch die regelmäßigen Betriebsausgaben ins Gewicht. Ein lokaler Server verursacht fortlaufende Kosten für Strom, Wartung, Kühlung und Updates. Die Höhe dieser Ausgaben richtet sich nach der Firmengröße, der Nutzerzahl und der benötigten Serverleistung. Kleine Firmen ohne IT-Abteilung benötigen externe Hilfe für den Support, was die Ausgaben steigert. Cloud-Dienste berechnen diese Aufwendungen bereits in den Abopreisen, weshalb Firmen keine einzelnen Wartungsgebühren zahlen müssen. Die Ausgaben lassen sich dadurch besser kalkulieren, und außerdem sinkt das Ausfallrisiko durch teure Reparaturen. Allerdings müssen sich Unternehmen bei Cloud-Diensten an die Preise des Anbieters halten; steigende Gebühren führen oft zu höheren Gesamtkosten.

Lokale Server verursachen durch einmalige Investitionen und feste Betriebskosten besser planbare Langzeitaufwendungen als die flexible, aber teurere Cloud-Alternative. Webgehostete Dienste passen IT-Ressourcen nach Bedarf an, ohne dass Hardwarekäufe erforderlich sind. Diese Anpassungsfähigkeit bringt kurzfristige Kostenvorteile, doch auf Dauer steigen die Ausgaben für Speicher und Leistung stetig. Die Unternehmen sollten deshalb abwägen, ob sich hohe Anfangskosten mit dauerhafter Kostenstabilität oder ein verbrauchsorientiertes System mit späteren Preiserhöhungen wirtschaftlich mehr lohnt.

3.2.3 ROI-Betrachtung

Die Rentabilität einer IT-Investition zeigt sich im ROI (Return of Invest). Der ROI gibt Auskunft über die Amortisationszeit der IT-Infrastruktur und den wirtschaftlichen Nutzen. Die Wahl zwischen lokalen Servern und Web-Services führt zu unterschiedlicher Kapitalbindung. Ein lokaler Server erfordert große Vorabinvestitionen mit Nutzen über Jahre, während Cloud-Dienste niedrige Startkosten haben. Diese können jedoch auf Dauer teuer werden. Die ROI-Analyse umfasst sowohl direkte Kosten als auch Vorteile, wie

⁴⁴ Cameron Fisher, „Cloud versus On-Premise Computing“, *American Journal of Industrial and Business Management* 8, Nr. 9 (4. September 2018): 1991–2006, <https://doi.org/10.4236/ajibm.2018.89133>.

bessere Abläufe, Kostensenkungen durch Automatisierung oder die Flexibilität der gewählten Option⁴⁵.

Neben den Investitionskosten haben mehrere betriebliche Faktoren Einfluss auf die Rentabilität einer IT-Infrastruktur. Unternehmen mit lokalen Servern nutzen feste und planbare Kosten sowie die volle Kontrolle über ihre IT-Systeme. Die Kosten für Wartung Updates und Strom belasten jedoch das Budget und verzögern den ROI. Webgehostete Services ermöglichen eine schnelle Amortisation, weil keine großen Anfangsinvestitionen nötig sind. Außerdem stehen IT-Ressourcen direkt zur Verfügung. Die Rentabilität auf lange Sicht hängt von den Preisen der Abonnementmodelle ab. Besonders Firmen mit steigendem IT-Bedarf müssen höhere Gebühren in ihre Planung aufnehmen. Diese Kosten reduzieren oft den frühen Preisvorteil von Cloud-Diensten⁴⁶. Tabelle 9 zeigt eine ROI-Berechnung für beide Systeme mit Beispielwerten über fünf Jahre. Angenommen werden Anfangsinvestitionen von 8.000,00€ für einen lokalen Server.

Zeitraum	Lokale Server (ROI in €)	Webgehostete Services (ROI in €)
Jahr 1	-8.000 €	-1.500 €
Jahr 2–3	-5.500 €	500 €
Jahr 4–5	1.500 €	2.500 €
Langfristiger ROI	3.500 €	1.500 €

Tabelle 9: ROI-Vergleich zwischen lokalen Servern und webgehosteten Services über verschiedene Zeiträume

Die Analyse ergibt, dass webgehostete Services schnell rentabel sind, weil die Kostenstruktur keine großen Anfangsinvestitionen benötigt. Ein lokaler Server erweist sich auf lange Sicht als günstiger, besonders wenn ein Unternehmen gleichbleibende IT-Anforderungen sowie feste Betriebskosten aufweist. Die ROI-Berechnung basiert nicht allein auf der Anfangsinvestition, sondern ebenso auf der Kostenentwicklung über Zeit als auch auf der tatsächlichen Nutzung der IT-Systeme. Firmen mit Bedarf an flexibler

⁴⁵ Sanjay Mohapatra und Laxmikant Lokhande, *Cloud Computing and ROI: A New Framework for IT Strategy*, Management for Professionals (Cham: Springer International Publishing, 2014), <https://doi.org/10.1007/978-3-319-08663-7>.

⁴⁶ Mohapatra und Lokhande.

Anpassung profitieren von Cloud-Diensten. Dagegen bevorzugen Firmen mit konstanter IT-Nutzung oft die Planungssicherheit eines eigenen Servers.

3.3 Organisatorische Machbarkeit

Die Einführung webgehosteter Services in Klein- und Kleinstunternehmen braucht eine gute Planung sowie eine stufenweise Umsetzung. Die technischen oder organisatorischen Faktoren bestimmen den Erfolg der Umstellung - dazu gehören Umstellungszeit, Schulungen und Prozessanpassungen. Ein passender Zeitplan und Schulungen der Mitarbeiter reduzieren Produktivitätsverluste als auch Widerstände innerhalb des Kollegiums.

3.3.1 Implementierungszeit & Aufwand

Die Zeit für die Umstellung auf webgehostete Services hängt von der Unternehmensgröße, der IT-Struktur und den spezifischen Anforderungen des Betriebs ab. Kleine Unternehmen mit geringerer IT-Abhängigkeit können die Migration in wenigen Wochen durchführen. Mittelständische Unternehmen oder Betriebe mit spezialisierten Anwendungen benötigen für die vollständige Integration mehrere Monate. Der Zeitrahmen wird auch durch die Art der Migration bestimmt: Ein stufenweiser Übergang zur Cloud gewährleistet die Stabilität des Betriebs, verlängert jedoch die Gesamtdauer des Projekts⁴⁷. Tabelle 10 zeigt ein typisches Anwendungsbeispiel in einem Kleinstunternehmen.

Phase	Dauer	Aktivitäten
Vorbereitung & Analyse	1–2 Wochen	Bestandsaufnahme der IT-Infrastruktur, Auswahl eines Cloud-Anbieters
Testmigration & Pilotbetrieb	2–4 Wochen	Datenübertragung für erste Nutzergruppen, Testphase mit Feedbackschleifen
Schrittweise Migration	4–6 Wochen	Übertragung der gesamten Datenbank, Integration der Cloud-Software

⁴⁷ Chitra Sabapathy Ranganathan und Rajeshkumar Sampathrajan, „Cloud Migration Meets Targeted Deadlines“, in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2023, 672–76, <https://doi.org/10.1109/ICESC57686.2023.10193104>.

Schulung & Anpassung	2–4 Wochen	Mitarbeiterschulung, Einführung von Sicherheitsrichtlinien
Abschluss & Optimierung	2 Wochen	Systemüberprüfung, Fehlerbehebung, finale Konfiguration

Tabelle 10: Phasen und Zeitrahmen der Migration zu webgehosteten Services

Eine frühzeitige Systemanalyse sowie eine schrittweise Migration helfen, Betriebsunterbrechungen zu minimieren und einen reibungslosen Übergang zu gewährleisten. Kleinere Unternehmen mit geringeren IT-Systemabhängigkeiten können den Umstieg oft in wenigen Wochen realisieren⁴⁸. Sie integrieren Cloud-Dienste zunächst als Ergänzung und wechseln nach erfolgreichen Tests zur neuen Infrastruktur. Die Entscheidung für einen schnellen oder schrittweisen Wechsel hängt von der Risikobereitschaft des Unternehmens sowie den Verfügbarkeitsanforderungen der Systeme ab.

3.3.2 Schulungsbedarf & Ressourcen

Ein zentraler Faktor für eine erfolgreiche Migration ist die Qualifikation der Mitarbeiter. IT-Abteilungen verfügen in der Regel über das technische Know-how für die Umstellung, jedoch benötigen andere Unternehmensbereiche Schulungen für die Nutzung der neuen Tools. Fehlende Schulung kann zu Widerständen, ineffizienter Nutzung und Sicherheitsrisiken führen. Der Schulungsaufwand hängt vom Ausmaß der Veränderung ab. Bei einem Wechsel von einer lokalen Serverstruktur zu cloudbasierten Systemen sind umfangreichere Schulungsmaßnahmen erforderlich. In Unternehmen mit hybriden Lösungen gestaltet sich der Übergang leichter, da bestehende Prozesse erhalten bleiben. Die Mitarbeiter:innen lernen den Umgang mit neuen Zugriffsrechten, Datensynchronisation und Cloud-Sicherheitsrichtlinien. Besonders wichtig sind Schulungen zu Datenzugriff, Dateiverwaltung und Sicherheitsprotokollen, da falsche Nutzung zu Datenschutzverletzungen führen kann⁴⁹.

Eine bewährte Strategie ist die Einführung von Train-the-Trainer-Programmen bei denen Key-User lernen ihr Wissen an Kolleginnen und Kollegen zu vermitteln. Das verringert die Bindung an externe Schulungsanbieter sowie ermöglicht dauerhafte Unterstützung im Unternehmen. Tabelle 11 zeigt die Schulungsthemen und den typischen Zeitaufwand pro Mitarbeiter:

⁴⁸ Zhixiao Wang, Wenyao Yan, und Wendong Wang, „Revisiting Cloud Migration: Strategies and Methods“, *Journal of Physics: Conference Series* 1575, Nr. 1 (Juni 2020): 012232, <https://doi.org/10.1088/1742-6596/1575/1/012232>.

⁴⁹ Lawrence E. Meyer und E. Billionniere, „Upskilling to Meet Cloud Talent Needs“, *2021 ASEE Virtual Annual Conference*, Juli 2021, <https://par.nsf.gov/biblio/10288742-upskilling-meet-cloud-talent-needs>.

Schulungsbereich	Zielgruppe	Dauer
Grundlagen der Cloud-Nutzung	Alle Mitarbeiter	2–4 Stunden
Datensicherheit & DSGVO	Führungskräfte, IT-Team	4–6 Stunden
Zugriffskontrolle & Berechtigungen	IT-Administratoren	1 Tag
Effiziente Nutzung von Cloud-Tools	Endanwender	2–3 Stunden

Tabelle 11: Schulungsplan für die Einführung webgehosteter Services

Ein strukturiertes Schulungskonzept fördert die Akzeptanz neuer Cloud-Infrastrukturen im Unternehmen. Eine Kombination aus Online-Schulungen, interaktiven Workshops und praxisnahen Trainings führt die Mitarbeitenden schrittweise an die neuen Systeme heran. Die Teilnehmer lernen dabei die Funktionen kennen, befolgen Sicherheitsrichtlinien und passen ihre Arbeitsprozesse an. Unternehmen, die gezielt in Schulungen investieren, erreichen eine schnelle Einarbeitung der Mitarbeiter und verringern Unsicherheiten im Umgang mit den neuen Technologien. Ein durchdachtes Schulungsprogramm unterstützt die technische Umsetzung und erleichtert die Integration in den Arbeitsalltag.

3.3.3 Anpassbarkeit & Benutzerfreundlichkeit

Die Anpassbarkeit von webgehosteten Services ist ausschlaggebend für die Integration in bestehende Geschäftsprozesse. Ein zentraler Vorteil dieser Lösungen ist die Modularität, die es Unternehmen ermöglicht, Funktionen auszuwählen und an spezifische Bedürfnisse anzupassen. Lokale Server bieten meist eine feste IT-Struktur, während Cloud-Dienste verschiedene Einstellungen für betriebliche Prozesse und Arbeitsabläufe bieten. Eine zu stark modifizierte Cloud-Umgebung kann jedoch zu zusätzlicher Verwaltungsarbeit führen. Besonders Kleinstunternehmen müssen daher einen Mittelweg zwischen Anpassungen und einfacher Bedienung finden, um die Arbeit nicht zu erschweren.

Ein wichtiger Aspekt für die Bedienbarkeit ist der einfache Umgang mit den neuen Systemen. Das Personal benötigt nur kurze Zeit für die Einarbeitung in die neue Technik.

Systeme mit einer klar strukturierten Benutzeroberfläche und verständlichen Menüs erleichtern den Wechsel und fördern die Akzeptanz⁵⁰. Die Integration in bestehende Tools ist von großer Bedeutung. Systeme, die gut mit E-Mail, Dokumenten oder Buchhaltungssoftware zusammenarbeiten, machen den Übergang einfacher. Eine Cloud-Software mit einer völlig neuen Benutzerumgebung führt häufig zu Widerständen und höherem Schulungsbedarf. Unternehmen sollten daher frühzeitig testen, ob die ausgewählte Lösung mit den bestehenden Systemen kompatibel ist. So wird der Umstieg für alle Mitarbeiter einfacher.

Trotz der Vorteile bringen Anpassungen oder Benutzerfreundlichkeit manchmal Herausforderungen. Standardisierte Cloud-Dienste bieten zwar einfache Konfigurationen haben aber begrenzte Individualisierungsmöglichkeiten. Ein Unternehmen mit besonderen Anforderungen muss entscheiden, ob es eine komplett angepasste Lösung braucht oder eine Standard-Plattform genügt. Die Sicherheit spielt dabei eine zentrale Rolle: Bei flexibleren Cloud-Lösungen wird eine präzise Festlegung von Zugriffsrechten nötig. Firmen mit Bedarf an hoher Kontrolle finden in Hybridlösungen oft eine passende Option, weil diese flexiblen Cloud-Dienste neben der Sicherheit lokaler Infrastruktur nutzen. Die Anpassungsfähigkeit von Web-Services muss deshalb immer zusammen mit wirtschaftlichen Zielen sowie der IT-Strategie bewertet werden.

⁵⁰ Juyeon Park und Marilyn DeLong, „User Perceptions of Technology Adoption and Implementation: A Case Study of Footwear Production in a Global Market“, *Fashion Practice* 1, Nr. 1 (1. Mai 2009): 87–108, <https://doi.org/10.2752/175693809X418865>.

4. Analyse Datenschutz & Datensicherheit

Die Migration von lokalen Servern zu webgehosteten Services stellt Datenschutz und Sicherheit vor neue Herausforderungen. Cloud-Dienste bieten moderne Schutzmaßnahmen, doch Fragen zu Compliance, Zugriffskontrolle und Risikomanagement bleiben. Diese Analyse betrachtet DSGVO-Anforderungen, Sicherheitskonzepte, Risiken sowie Backup- und Wiederherstellungslösungen, um eine fundierte Entscheidungsgrundlage zu schaffen.

4.1 Einhaltung der DSGVO

Die DSGVO regelt den Schutz personenbezogener Daten und stellt Anforderungen an deren Verarbeitung und Speicherung. Unternehmen mit webgehosteten Services müssen sicherstellen, dass ihre Cloud-Anbieter DSGVO-konform arbeiten, insbesondere bei Datenhoheit, Zugriffskontrollen und Verschlüsselung. Regelmäßige Prüfungen und vertragliche Vereinbarungen helfen, Verstöße und Datenpannen zu vermeiden.

4.1.1 Grundlagen & Anforderungen

Die DSGVO legt fest, was Unternehmen bei der Verarbeitung von personenbezogenen Daten beachten müssen. Die Regeln gelten sowohl für das Speichern als auch für die Verarbeitung von Daten und deren Schutz. Bei Unternehmen mit lokalen Servern bleibt die Kontrolle über die IT-Systeme in der eigenen Hand. Bei webgehosteten Diensten hingegen müssen Unternehmen sich nach den Schutzkonzepten des Anbieters richten. Bei der Auswahl eines Cloud-Dienstes muss ein Unternehmen auf die DSGVO-Konformität achten. Der Anbieter sollte ausreichende Mechanismen zum Schutz personenbezogener Daten vorweisen. Eine gründliche Analyse des Cloud-Anbieters sowie seiner Zertifikate hilft, Verstöße gegen den Datenschutz zu vermeiden⁵¹.

Ein weiterer wesentlicher Aspekt der DSGVO ist die Datenhoheit und der Speicherort der Daten. Unternehmen, die mit lokalen Servern arbeiten, können den physischen Speicherort genau bestimmen und Sicherheitsmaßnahmen individuell festlegen. Cloud-Dienste speichern Daten häufig in verteilten Rechenzentren, die sich in unterschiedlichen Ländern befinden können. Dies führt zu rechtlichen Herausforderungen, insbesondere wenn Daten außerhalb der EU verarbeitet werden. Unternehmen müssen daher vertraglich sicherstellen, dass die Daten entweder innerhalb der EU verbleiben oder durch Mechanismen wie Standardvertragsklauseln oder spezielle Vereinbarungen mit

⁵¹ Becker u. a., „Applying GDPR roles and responsibilities to scientific data sharing“.

dem Cloud-Anbieter abgesichert sind. Die Kontrolle über Datenflüsse ist ein wesentlicher Punkt für die Einhaltung der Datenschutzvorgaben⁵².

Zusätzlich zur Speicherung regelt die DSGVO auch die Datensicherheit im Betrieb. Unternehmen müssen technische und organisatorische Maßnahmen ergreifen, um unbefugten Zugriff sowie Datenverlust zu verhindern. Lokale IT-Abteilungen setzen eigene Verschlüsselungs- und Zugriffskontrollmechanismen um, während Cloud-Anbieter diese Maßnahmen bereitstellen. In den Verträgen müssen klare Schutzmaßnahmen des Anbieters festgelegt werden, ebenso wie die Kontrollmöglichkeiten für die Kunden. Eine klare Sicherheitsstrategie ist ausschlaggebend, um Datenschutzverstöße zu vermeiden und die Anforderungen der DSGVO zu erfüllen⁵³.

Anforderung	Lokale Server	Webgehostete Services
Datenhoheit	Volle Kontrolle	Abhängig vom Anbieter
Verarbeitungsverträge	Nicht erforderlich	Muss mit Cloud-Anbieter abgeschlossen werden
Speicherort	Lokales Rechenzentrum	Oft in internationalen Serverfarmen
Sicherheitsmaßnahmen	Individuell festlegbar	Standardisierte Sicherheitsrichtlinien

Tabelle 12: Vergleich der Datenschutz- und Sicherheitsanforderungen zwischen lokalen Servern und webgehosteten Services

4.1.2 Betroffenenrechte & Transparenz

Die DSGVO gewährt den Menschen weitreichende Rechte zum Schutz ihrer persönlichen Daten. Unternehmen müssen Verfahren für den Datenzugriff, Korrekturen oder Löschungen etablieren. Bei lokalen Servern erfolgen diese Prozesse intern, während bei webgehosteten Services der Anbieter die technische Umsetzung steuert. Eine komplexe Aufgabe stellt das Recht auf Datenübertragung dar, da Daten in einem strukturierten

⁵² Nemer Alberto Zaguir, Guilherme Henrique de Magalhães, und Mauro de Mesquita Spinola, „Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions“, *IEEE Access* 12 (2024): 81608–30, <https://doi.org/10.1109/ACCESS.2024.3406724>.

⁵³ Maria Addis und Maria Kutar, „The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness“, *UK Academy for Information Systems Conference Proceedings 2018*, 20. März 2018, <https://aisel.aisnet.org/ukais2018/29>.

Format vorliegen müssen. Dies führt bei Cloud-Diensten, die eigene Datenformate verwenden, zu Schwierigkeiten. Fehlende Exportfunktionen im Standardformat erschweren die Umsetzung darüber hinaus⁵⁴.

Ein weiterer Aspekt ist die Transparenz der Datenverarbeitung. Unternehmen müssen betroffenen Personen klar darlegen, wie sie deren Daten verarbeiten. Bei lokalen Servern lässt sich dies direkt vom Unternehmen steuern, doch Cloud-Dienste benötigen zusätzliche Prüfmechanismen. Anbieter brauchen Dokumentationen sowie Datenschutzrichtlinien, die den gesetzlichen Vorgaben entsprechen. Die Unternehmen prüfen in festen Abständen die Vollständigkeit der Informationen, da neue Datenschutzbestimmungen der Anbieter die DSGVO-Konformität verändern können⁵⁵.

Zudem nimmt die Protokollierung von Zugriffen und Änderungen bei personenbezogenen Daten eine zentrale Rolle für die Transparenz ein. Unternehmen mit eigenen Servern behalten die vollständige Kontrolle über Log-Dateien, während Cloud-Dienste sich an die Protokollvorgaben des Anbieters halten müssen. Solche Beschränkungen erschweren interne Prüfungen und Audits, besonders wenn die Zugriffsdaten nicht detailliert genug vorliegen. Daher sollten Unternehmen in Verträgen festlegen, dass sie über ausreichende Logging- und Monitoring-Funktionen verfügen, um ihrer Rechenschaftspflicht gerecht zu werden⁵⁶.

4.2 Sicherheitsstrategien & Maßnahmen

Ganzheitliche Sicherheitsstrategien schützen Daten vor Cyberangriffen, unbefugtem Zugriff und Datenverlust. Unternehmen setzen Verschlüsselungstechniken, Zugriffskontrollsysteme und Intrusion-Detection-Systeme ein, um sensible Informationen zu schützen. Regelmäßige Sicherheitsüberprüfungen sowie Notfallpläne decken Schwachstellen auf und ermöglichen schnelle Gegenmaßnahmen.

4.2.1 Verschlüsselung & Zugriffskontrollen

Die Verschlüsselung sensibler Daten ist ein zentraler Bestandteil der IT-Sicherheit und schützt vor Datendiebstahl. Traditionelle lokale Server setzen auf AES-256-Verschlüsselung u.a. in Kombination mit Hardware-Sicherheitsmodulen (HSMs). Cloud-Dienste bieten unterschiedliche Verschlüsselungsmethoden, darunter clientseitige und

⁵⁴ He Li, Lu Yu, und Wu He, „The Impact of GDPR on Global Technology Development“, *Journal of Global Information Technology Management* 22, Nr. 1 (2. Januar 2019): 1–6, <https://doi.org/10.1080/1097198X.2019.1569186>.

⁵⁵ Eva Schlehahn und Rigo Wenning, „GDPR Transparency Requirements and Data Privacy Vocabularies“, in *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, hg. von Eleni Kosta u. a. (Cham: Springer International Publishing, 2019), 95–113, https://doi.org/10.1007/978-3-030-16744-8_7.

⁵⁶ Theo Lynn, „Dear Cloud, I Think We Have Trust Issues: Cloud Computing Contracts and Trust“, in *Data Privacy and Trust in Cloud Computing: Building Trust in the Cloud through Assurance and Accountability*, hg. von Theo Lynn u. a. (Cham: Springer International Publishing, 2021), 21–42, https://doi.org/10.1007/978-3-030-54660-1_2.

serverseitige Verfahren sowie homomorphe Verschlüsselung. Zur sicheren Verwaltung von Verschlüsselungsschlüsseln stellen Anbieter wie AWS, Azure und Google Cloud spezielle Key Management Services (KMS) bereit, darunter AWS KMS, Azure Key Vault und Google Cloud KMS.

Neben der Verschlüsselung sind wirksame Zugriffskontrollen essenziell, um sensible Systeme und Daten zu schützen. IAM (Identity and Access Management) bildet das Fundament moderner Sicherheitskonzepte und steuert die detaillierte Rechtevergabe auf Basis von Rollen und Attributen. Zero-Trust-Modelle überwachen Zugriffe kontinuierlich und beschränken sie auf das erforderliche Minimum. Cloud-Dienste wie AWS IAM, Azure Active Directory und Google Cloud IAM ermöglichen eine flexible Zugriffskontrolle, bei der Berechtigungen dynamisch anhand von Standort, Nutzungsmustern und Risikobewertungen angepasst werden⁵⁷. Die Kombination aus MFA und automatisierten Prüfungen der Zugriffsrechte erhöht die Sicherheit und unterstützt die Einhaltung regulatorischer Vorgaben.

Die Kombination aus Verschlüsselung und Zugriffskontrollen bildet ein starkes Sicherheitsfundament. Unternehmen sollten regelmäßige Audits, Schwachstellenanalysen und Penetrationstests durchführen, um Sicherheitslücken frühzeitig zu erkennen. AI-gestützte Anomalie Erkennung, automatisierte Berechtigungsverwaltung und Echtzeit-Monitoring ermöglichen die Identifikation verdächtiger Zugriffe und das proaktive Stoppen von Angriffen. Klare Sicherheitsrichtlinien für Drittanbieter stellen sicher, dass externe Partner verschlüsselte Verbindungen und strenge Zugriffskontrollen nutzen. Durch die kontinuierliche Weiterentwicklung von Verschlüsselungs- und Zugriffskontrollsystemen bleiben Unternehmensdaten langfristig geschützt und Compliance-Vorgaben erfüllt.

4.2.2 Netzwerksicherheit & Firewalls

Netzwerksicherheit schützt die vertraulichen Daten von Unternehmen, besonders in der Cloud. Klassische IT-Systeme verwenden physische Firewalls an den Netzwerkezugängen. In der Cloud kommen jedoch verbesserte Schutzmechanismen zum Einsatz, wie softwarebasierte Firewalls und Zero-Trust-Modelle. Eine Cloud-Firewall verwaltet Sicherheitsregeln zentral für verschiedene Standorte und schützt vor neuen Angriffen durch regelmäßige Updates. Das Prinzip der Mikrosegmentierung unterteilt Cloud-Systeme in separate Schutzzonen und kontrolliert den Datenfluss präzise. Dieses System begrenzt die seitliche Ausbreitung von Angriffen im Netzwerk und schützt kritische Unternehmensbereiche vor unbefugtem Zugriff⁵⁸.

⁵⁷ Kabiru Hamza Mohammed, Abubakar Hassan, und Danlami Yusuf Mohammed, „Identity and Access Management System: A Web-Based Approach for an Enterprise“, 2018, <http://oer.udusok.edu.ng:8080/xmlui/handle/123456789/837>.

⁵⁸ Poonam Dhiman u. a., „A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model“, *Sensors* 24, Nr. 4 (Januar 2024): 1328, <https://doi.org/10.3390/s24041328>.

Ein wesentlicher Unterschied zwischen lokalen- und Cloud-Sicherheitsarchitekturen zeigt sich beim Einsatz von Intrusion Detection und Prevention Systemen (IDS/IPS) sowie Sicherheitsinformations- und Ereignismanagementsysteme (SIEM)-Lösungen. Klassische IDS/IPS-Systeme analysieren den Netzwerkverkehr und blockieren Angriffe anhand vordefinierter Signaturen. Moderne Cloud-SIEM-Plattformen hingegen nutzen künstliche Intelligenz und maschinelles Lernen, um Anomalien in Echtzeit zu erkennen. Dieser Ansatz ermöglicht eine dynamische Bedrohungserkennung, die sowohl bekannte als auch neue Angriffsmuster identifiziert. Unternehmen, die Cloud-Dienste nutzen, benötigen einen Anbieter, der sowohl SIEM- als auch SOAR-Technologien (Security Orchestration Automation and Response) für eine proaktive Sicherheitsstrategie bereitstellt⁵⁹.

Die Wahl einer passenden Netzwerksicherheitsstrategie richtet sich nach den Bedürfnissen eines Unternehmens. Eine Verbindung von bewährten Schutzmaßnahmen wie Firewalls, sowie moderne Cloud-Sicherheitslösungen, schafft guten Schutz vor Cyberbedrohungen. Tabelle 13 zeigt zentrale Merkmale von traditionellen oder cloudbasierten Sicherheitsarchitekturen:

Sicherheitsfaktor	Traditionelle IT	Cloud-Sicherheit
Firewall-Implementierung	Hardware-Firewalls am Netzwerk-Gateway	Softwaredefinierte Firewalls mit globaler Steuerung
Bedrohungserkennung	Signaturbasierte IDS/IPS-Systeme	KI-gestützte Echtzeitanalyse mit SIEM
Zugriffskontrolle	Manuelle Berechtigungsverwaltung	Zero-Trust-Modelle mit Mikrosegmentierung
Skalierbarkeit	Begrenzte physische Ressourcen	Dynamische Anpassung an den Datenverkehr
Incident Response	Lokale IT-Abteilungen verwalten Sicherheitsvorfälle	Automatisierte Reaktion durch SOAR-Technologien

⁵⁹ Maria Papadaki und Steven Furnell, „IDS or IPS: what is best?“, *Network Security* 2004, Nr. 7 (1. Juli 2004): 15–19, [https://doi.org/10.1016/S1353-4858\(04\)00106-0](https://doi.org/10.1016/S1353-4858(04)00106-0).

Tabelle 13: Vergleich der Sicherheitsmaßnahmen zwischen traditioneller IT und Cloud-Sicherheit

Unternehmen mit Cloud-basierter Netzwerksicherheit nutzen eine anpassbare Schutzinfrastruktur. Die Systeme müssen jedoch transparent bleiben, sowohl für Kontrollen als auch für Bedrohungen. Ein Mix aus lokalen Schutzmaßnahmen für wichtige Systeme und Cloud-Lösungen für weniger sensible Prozesse schafft ein gutes Gleichgewicht in der Sicherheit.

4.3 Risikoanalyse & Schwachstellenbewertung

Eine Risikoanalyse erkennt Bedrohungen für IT-Systeme und bewertet deren Auswirkungen auf die Datensicherheit. Regelmäßige Schwachstellenbewertungen ermöglichen die frühzeitige Identifikation von Sicherheitslücken und gezielte Schutzmaßnahmen. Bedrohungsmodelle und automatisierte Analysetools stärken die Sicherheitsinfrastruktur und reduzieren das Risiko von Cyberangriffen.

4.3.1 Identifikation & Bewertung von Risiken

Die Erkennung von IT-Sicherheitsrisiken erfordert eine Analyse der Gefahren von innen und außen. Firmen müssen neben Malware, Phishing und DDoS-Attacken auch die Risiken der Cloud-Nutzung berücksichtigen. Dazu gehören falsche Cloud-Einstellungen, offene APIs, Datenverluste durch mangelhafte Zugriffskontrolle sowie die Bindung an bestimmte Anbieter. Ein wirksamer Schutz erfordert regelmäßige Tests der Netzwerke, Datenverbindungen und Berechtigungen, um Lücken frühzeitig zu identifizieren und zu beheben⁶⁰.

Die Bewertung dieser Risiken basiert auf mehreren Kriterien wie der Eintrittswahrscheinlichkeit eines Vorfalls und seinen Folgen für den Geschäftsbetrieb. Unternehmen nutzen Risikomatrizen zur Einstufung von Bedrohungen nach Kritikalität und ordnen Gegenmaßnahmen Vorrang zu⁶¹. Hochkritische Risiken wie ein umfangreicher Datenverlust oder ein Sicherheitsverstoß mit Kundendaten benötigen unmittelbare Gegenmaßnahmen. Die weniger kritischen Risiken erfordern ebenfalls Aufmerksamkeit. Tabelle 14 zeigt eine strukturierte Bewertung von Bedrohungen sowie entsprechenden Schutzmaßnahmen.

⁶⁰ Aiman Al-Sabaawi und Thamer A. Alrowidhan, „Detecting Network Security Vulnerabilities and Proactive Strategies to Mitigate Potential Threats“ (arXiv, 22. Dezember 2022), <https://doi.org/10.48550/arXiv.2212.11449>.

⁶¹ Michael Krisper, „Problems with Risk Matrices Using Ordinal Scales“ (arXiv, 7. März 2021), <https://doi.org/10.48550/arXiv.2103.05440>.

Risiko	Wahrscheinlichkeit	Auswirkung	Empfohlene Gegenmaßnahmen
Cloud-Fehlkonfiguration	Hoch	Kritisch	Automatisierte Compliance-Prüfung
API-Sicherheitslücken	Mittel	Hoch	Zugriffsbeschränkungen & Monitoring
Insider-Bedrohungen	Gering	Mittel	Zero-Trust-Zugriffsmodell
DDoS-Angriffe	Hoch	Mittel	Skalierbare Cloud-Firewalls

Tabelle 14: Risikobewertung und empfohlene Gegenmaßnahmen für Cloud-Sicherheit

Zur Risikominderung empfehlen sich KI-gestützte Bedrohungsanalysen und automatische Angriffserkennung. Die Cloud-Sicherheitslösungen nutzen verhaltensbasierte Systeme zur Analyse ungewöhnlicher Aktivitäten und deren Risikobewertung in Echtzeit. Unternehmen müssen ihre Sicherheitsrichtlinien an neue Bedrohungen anpassen und ihre Mitarbeiter regelmäßig schulen. Ein strukturiertes Risikomanagement erkennt Bedrohungen frühzeitig und reduziert sie durch gezielte Maßnahmen, sodass die Widerstandsfähigkeit des Unternehmens gesteigert wird.

4.3.2 Bedrohungsmodelle & Schutzmaßnahmen

Die Bedrohungsmodellierung bildet einen wichtigen Teil der Sicherheitsstrategie und unterstützt die Identifikation von Angreifern, Methoden sowie Angriffswegen. Bewährte Modelle wie STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) ermöglichen eine präzise Analyse der IT-Schwachstellen in lokalen Systemen⁶². Die Cloud-Umgebung bringt eigene Risiken mit sich – etwa API-Sicherheitslücken, Fehlkonfigurationen, Angriffe auf Container-Systeme und Datenverlust durch Anbieterabhängigkeit. Aktuelle Cloud-Sicherheitskonzepte nutzen CLOUD

⁶² Dimitri Van Landuyt und Wouter Joosen, „A Descriptive Study of Assumptions in STRIDE Security Threat Modeling“, *Software and Systems Modeling* 21, Nr. 6 (1. Dezember 2022): 2311–28, <https://doi.org/10.1007/s10270-021-00941-7>.

STRIDE oder das MITRE ATT&CK-Framework, um Bedrohungen in verteilten Systemen zu analysieren und passende Schutzmaßnahmen zu entwickeln⁶³.

Die Auswahl passender Schutzmaßnahmen basiert auf der Art der bekannten Bedrohungen. Die klassische IT-Sicherheit nutzt Firewalls, Intrusion Detection Systems (IDS) und MFA. In Cloud-Umgebungen sind jedoch zusätzliche Sicherheitsmechanismen erforderlich. Eine Zero-Trust-Architektur ist ein wesentlicher Baustein, ebenso wie das IAM für Cloud-Dienste. Die Sicherheitsüberwachung erfolgt durch SIEM sowie SOAR⁶⁴. Eine Kombination aus Verhaltensanalyse und maschinellem Lernen ermöglicht die frühe Erkennung von Bedrohungen und löst automatische Gegenmaßnahmen aus. Tabelle 15 stellt traditionelle sowie cloudbasierte Schutzmaßnahmen gegenüber.

Schutzmaßnahme	Traditionelle IT-Sicherheit	Cloud-Sicherheit
Bedrohungsmodell	STRIDE, DREAD	CLOUD STRIDE, MITRE ATTACK
Zugriffsverwaltung	Klassische Rechtevergabe	Zero-Trust-Architektur
Bedrohungserkennung	Signaturbasierte IDS/IPS	KI-gestützte Anomalieerkennung
Datenverschlüsselung	Festplattenverschlüsselung	End-to-End-Cloud-Verschlüsselung
Incident Response	Manuelle Sicherheitsüberprüfung	Automatisierte SOAR-Reaktionen

Tabelle 15: Vergleich von Schutzmaßnahmen zwischen traditioneller IT-Sicherheit und Cloud-Sicherheit

Neben den technischen Schutzmaßnahmen sind regelmäßige Tests der Bedrohungsmodelle notwendig, damit Unternehmen neue Angriffsmethoden abwehren können. Eine Organisation sollte Penetrationstests durchführen, um Schwachstellen frühzeitig zu erkennen und die Abwehr zu verbessern. Der Einsatz von Threat Intelligence-Plattformen hilft dabei, aktuelle Bedrohungen zu erfassen und in die Sicherheitsstrategie zu integrieren. Schulungen der Mitarbeiter zum Schutz vor Social Engineering, wie Phishing oder

⁶³ Mohamed Ahmed u. a., „MITRE ATT&CK-driven Cyber Risk Assessment“, in *Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22* (New York, NY, USA: Association for Computing Machinery, 2022), 1–10, <https://doi.org/10.1145/3538969.3544420>.

⁶⁴ Amir Azodi u. a., „A New Approach to Building a Multi-tier Direct Access Knowledgebase for IDS/SIEM Systems“, in *2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, 2013*, 118–23, <https://doi.org/10.1109/DASC.2013.48>.

Business E-Mail Kompromisse, bilden einen zentralen Bestandteil des Sicherheitskonzepts. Die kontinuierliche Anpassung der Regeln sowie der Austausch mit externen Experten führen zu einer besseren Abwehr von Cyberangriffen und stärken die IT-Infrastruktur.

4.4 Backup & Wiederherstellungsstrategien

Ein verlässliches System für Backup und Wiederherstellung schützt Daten bei Systemausfällen oder Cyberangriffen. Unternehmen nutzen lokale, cloudbasierte oder hybride Backup-Methoden, um eine Balance zwischen Sicherheit, Speicher und Wiederherstellungszeit zu gewährleisten. Regelmäßige Tests und automatisierte Wiederherstellungsprozesse sorgen dafür, dass Daten im Notfall schnell verfügbar sind.

4.4.1 Backup-Methoden & Speicherorte

Die Auswahl passender Backup-Methoden bestimmt die Qualität der Datensicherung und Wiederherstellung in Notfällen. Unternehmen nutzen vollständige, inkrementelle sowie differentielle Backups für verschiedene Anforderungen. Ein Vollbackup erstellt eine komplette Kopie der Daten und schützt diese optimal, benötigt jedoch viel Speicher und Zeit. Inkrementelle Backups erfassen nur neue Datenänderungen seit der letzten Sicherung. Dies spart Speicherplatz, verzögert jedoch die Wiederherstellung, da mehrere Sicherungen kombiniert werden müssen. Differentielle Backups bieten einen Mittelweg. Sie speichern alle Änderungen seit dem letzten Vollbackup, was die Wiederherstellung beschleunigt⁶⁵. Tabelle 16 zeigt den Vergleich dieser Methoden nach Speicherbedarf, Sicherungszeit und Dauer der Wiederherstellung.

⁶⁵ Zi Qiang Wu und Hui Li, „Analysis of Data Backup and Recovery System“, *Applied Mechanics and Materials* 631–632 (2014), <https://doi.org/10.4028/www.scientific.net/amm.631-632.1207>.

Backup-Methode	Speicherbedarf	Sicherungszeit	Wiederherstellungszeit
Vollbackup	Hoch	Lang	Schnell
Inkrementell	Niedrig	Kurz	Lang
Differentiell	Mittel	Mittel	Mittel

Tabelle 16: Vergleich der Backup-Methoden hinsichtlich Speicherbedarfes, Sicherungszeit und Wiederherstellungszeit

Der Speicherort ist genauso wichtig wie die Backup-Methode für die Datensicherheit. Lokale Backups auf Servern oder NAS-Systemen ermöglichen einen schnellen Zugriff auf gespeicherte Daten. Diese Systeme haben jedoch Schwächen bei Hardware-Defekten oder räumlichen Schäden. Cloud-Backups schützen die Daten besser durch verteilte Speicherung, automatische Redundanz sowie anpassbaren Speicherplatz. Unternehmen profitieren von Backup-as-a-Service durch automatische Sicherungen, geografisch verteilte Speicherung und zusätzliche Schutzfunktionen wie Verschlüsselung oder Zugriffskontrollen. Ein hybrides Backup-System mit lokalen und Cloud-Sicherungen ermöglicht einen schnellen Datenzugriff im Ernstfall und bietet Schutz vor physischen sowie digitalen Bedrohungen⁶⁶.

Die Backup-Strategie richtet sich nach dem Recovery Time Objective (RTO) und dem Recovery Point Objective (RPO); diese Werte legen die Dauer der Wiederherstellung sowie den akzeptablen Datenverlust fest. Unternehmen aus dem Finanz- oder Gesundheitssektor mit geringem RTO und RPO sollten Snapshot-Sicherungen in Kombination mit Kontinuierlicher Data Protektion nutzen, da sie den Datenverlust auf Sekunden reduzieren. Backup-Tests sowie Disaster-Recovery-Pläne müssen regelmäßig durchgeführt werden, damit Daten bei Bedarf schnell wiederhergestellt werden können. Eine Mischung aus verschiedenen Backup-Methoden, verteilten Speicherorten und automatischen Wiederherstellungsprozessen schafft eine widerstandsfähige Backup-Strategie, die aktuelle Sicherheits- und Compliance-Vorgaben erfüllt⁶⁷.

⁶⁶ Wu und Li.

⁶⁷ P. Fallara, „Disaster recovery planning“, *IEEE Potentials* 23, Nr. 5 (Dezember 2004): 42–44, <https://doi.org/10.1109/MP.2004.1301248>.

4.4.2 Notfallwiederherstellung & Redundanz

Eine gute Notfallwiederherstellung erfordert klare Pläne für lokale oder Cloud-Lösungen. Unternehmen setzen zunehmend auf Disaster Recovery as a Service, um eine schnelle Systemwiederherstellung mit minimalen Handeingriffen zu ermöglichen. Lokale Failover-Cluster mit zusätzlichen Rechenzentren sorgen für hohe Verfügbarkeit, während Cloud-Redundanz automatische Skalierung und geografisch verteilte Speicherung bietet. Die Cross-Region-Replikationen in Multi-Cloud-Systemen wie AWS Multi-AZ oder Google Cloud Persistent Disk Replication schützen vor regionalen Störungen. Die Kombination aus lokalen Systemen und Cloud-Strategien macht Unternehmen widerstandsfähig gegenüber physischen oder digitalen Ausfällen⁶⁸.

Redundanz bildet das Fundament für Hochverfügbarkeitslösungen und minimiert Ausfallzeiten durch zwei oder mehr parallel funktionierende Systeme. Unternehmen nutzen verschiedene Redundanzmodelle, die sich nach der Bedeutung ihrer Systeme richten – zum Beispiel Hot Standby, Cold Standby, Active-Active sowie Active-Passive Failover-Strukturen. Active-Active-Systeme teilen die Last gleichmäßig auf und ermöglichen einen unterbrechungsfreien Betrieb. Cold-Standby-Systeme erfordern dagegen eine manuelle Aktivierung mit längeren Zeiten bis zur Wiederherstellung⁶⁹. Tabelle 17 zeigt die Unterschiede der Redundanzstrategien auf.

Redundanzstrategie	Beschreibung	Vorteile	Nachteile
Active-Active	Parallellaufende Systeme mit Lastverteilung	Keine Verzögerung, hohe Verfügbarkeit	Höhere Kosten und Komplexität
Hot Standby	Ersatzsystem läuft im Hintergrund und übernimmt bei Ausfall sofort	Schnelle Übernahme, geringer Datenverlust	Erfordert hohe Ressourcen

⁶⁸ Steve M. Hawkins, David C. Yen, und David C. Chou, „Disaster recovery planning: a strategy for data security“, *Information Management & Computer Security* 8, Nr. 5 (1. Januar 2000): 222–30, <https://doi.org/10.1108/09685220010353150>.

⁶⁹ Siddharth Choudhary Rajesh, „High Availability Strategies in Distributed Systems: A Practical Guide“, *International Journal of Research in All Subjects in Multi Languages*, Nr. 13 (18. Januar 2025): 110–30.

Warm Standby	Ersatzsystem läuft mit reduzierter Kapazität und wird hochgefahren	Balance zwischen Kosten und Geschwindigkeit	Verzögerung bei Skalierung
Cold Standby	Ersatzsystem wird erst bei Bedarf hochgefahren	Kostengünstig	Lange Wiederherstellungszeit

Tabelle 17: Vergleich von Redundanzstrategien für Notfallwiederherstellung

Regelmäßige Tests und kontinuierliche Optimierung gewährleisten die Aktualität von Notfallwiederherstellungs- und Redundanzplänen. Unternehmen sollten Failover-Tests und Disaster-Recovery-Übungen durchführen, um die Reaktionszeiten und Effektivität ihrer Prozesse zu evaluieren. Erkenntnisse aus vergangenen Störungen tragen zur Entwicklung verbesserter Strategien bei. Eine enge Abstimmung mit Cloud- und Infrastrukturpartnern sowie der Einsatz von maschinellem Lernen zur Früherkennung von Systemausfällen und automatisierten Wiederherstellungsprozessen erhöhen die Resilienz gegenüber unvorhergesehenen Ausfällen. Diese Maßnahmen minimieren Betriebsunterbrechungen und sichern die Kontinuität geschäftskritischer Prozesse⁷⁰.

⁷⁰ Wasiq Noor Ahmad Qasmi u. a., „A comparative study of failover schemes for IaaS recovery“, in *2018 International Conference on Information Networking (ICOIN)*, 2018, 25–30, <https://doi.org/10.1109/ICOIN.2018.8343078>.

5. Auswertung & Zusammenfassung der Ergebnisse

Die durchgeführte Machbarkeitsstudie bestätigt die Machbarkeit der Umsetzung einer Migration zu webgehosteten Services aus technischer, wirtschaftlicher und organisatorischer Sicht, einschließlich der Sicherheitsaspekte. Die quantitative Analyse belegt eine bessere Systemverfügbarkeit, niedrigere Betriebskosten sowie verbesserte Skalierbarkeit im Vergleich zu lokalen Serverlösungen. Dies kann aus den ausgearbeiteten Punkten eindeutig abgeleitet werden. Die erwarteten Vorteile in Bezug auf Kosteneinsparungen und Automatisierungspotenziale wurden bestätigt. Dennoch ergaben sich neue Schwierigkeiten bei der Datenmigration, dem Integrationsaufwand sowie den regulatorischen Vorgaben. Die Tabelle 18 stellt die wesentlichen Erkenntnisse dar:

Bewertungskriterium	Ergebnis
Systemverfügbarkeit	Erhöht durch Cloud-Redundanz
Betriebskosten	Langfristig niedriger, jedoch anfängliche Implementierungskosten
Sicherheitsrisiken	Minimierbar durch starke Verschlüsselung und Zugriffsverwaltung
Akzeptanz & Schulung	Notwendig für effiziente Nutzung und Compliance

Tabelle 18: Bewertung der Notfallwiederherstellungs- und Redundanzstrategie

Die gewonnenen Erkenntnisse liefern eine gute Basis für künftige Entscheidungen zur Optimierung bzw. betriebsbedingten Migrationen in webgehostet Plattformen. Unternehmen müssen ihre spezifischen Anforderungen mit den untersuchten Vor- und Nachteilen vergleichen und abwägen, um die passende Wahl zwischen lokalen oder cloudbasierten Lösungen zu treffen.

6. Beantwortung der Forschungsfrage

Ist die Umstellung auf webgehostete Services für Unternehmen machbar?

Diese Machbarkeitsstudie zeigt, dass die Migration umsetzbar ist, wenn bestimmte technische, wirtschaftliche sowie organisatorische Bedingungen erfüllt sind. Eine stabile Internetverbindung und eine passende IT-Infrastruktur ermöglichen einen reibungslosen Übergang. Die wirtschaftlichen Vorteile überwiegen langfristig, durch niedrigere Betriebskosten und bessere Skalierbarkeit, trotz der anfänglichen Implementierungs- und Schulungskosten. Der Erfolg hängt von der Planung, von der Mitarbeiterakzeptanz sowie der Integration in bestehende Abläufe ab. Cloud-Dienste bieten neue Schutzmaßnahmen, erfordern jedoch klare Zugriffskontrollen und eine DSGVO-konforme Datenspeicherung.

Aus den Ergebnissen ergeben sich konkrete Handlungsempfehlungen für die Umstellung. Unternehmen mit wechselnden IT-Bedürfnissen oder veränderlicher Skalierung profitieren von Cloud-Systemen. Lokale Server bleiben für Branchen mit strengen Datenschutzvorgaben oder schwacher Internetverbindung eine geeignete Option. Die Entscheidung für Cloud- oder lokalen Serverlösungen muss sich an Sicherheitsrichtlinien, Geschäftsmodellen sowie der langfristigen Wirtschaftlichkeit orientieren. Ein gemischtes Konzept, das lokale kritische Systeme und Cloud-basierte Standardprozesse kombiniert, bietet vielen Unternehmen den besten Lösungsweg.

Die ausgearbeiteten Ergebnisse bilden eine Grundlage für strategische IT-Entscheidungen und bieten Ansatzpunkte für weiterführende Studien. Die Analyse der Langzeiteffekte von Cloud-Systemen auf Geschäftsprozesse sowie die Auswirkungen auf den Datenschutz eröffnen neue Forschungsfelder. Eine detaillierte Untersuchung der Migrationsstrategien nach Branchen ermöglicht gezielte Empfehlungen für jeden Bereich.

7. Zusammenfassung & Ausblick

Die Arbeit zeigt, dass Unternehmen auf webgehostete Services umstellen können, wenn sie technische, wirtschaftliche, organisatorische und datenschutzrelevante Faktoren berücksichtigen. Cloud-Technologie bietet bessere Skalierbarkeit, Kosteneinsparungen und verbesserte Sicherheitsmechanismen. Dennoch erfordert die erfolgreiche Umsetzung eine angepasste IT-Strategie. Zentrale Herausforderungen sind die Integration bestehender Systeme, die Einhaltung regulatorischer Vorgaben und die Schulung der Mitarbeitenden zur Sicherstellung einer hohen Akzeptanz. Zudem muss der Fokus auf der dauerhaften Datenhoheit liegen, damit Unternehmen die Kontrolle über kritische Geschäftsprozesse behalten und eine übermäßige Abhängigkeit von Cloud-Anbietern vermeiden.

Langfristig führt die Digitalisierung der IT-Infrastrukturen zu mehr betrieblicher Flexibilität und Wettbewerbsvorteilen, sofern Unternehmen die Migration strategisch planen. Die Wahl zwischen Cloud- und lokalen Serversystemen sollte sich an den individuellen Geschäftszielen orientieren, wobei hybride Lösungen zunehmend an Bedeutung gewinnen. Technische und organisatorische Herausforderungen lassen sich durch kontinuierliche Erfolgsmessungen und regelmäßige Anpassungen bewältigen. Eine moderne und sichere IT-Landschaft entsteht durch gezielte Prüfungen und Leistungsanalysen, die die Wirkung der Migration bewerten und notwendige Optimierungen aufzeigen.

Für die Forschung ergeben sich neue Fragestellungen zur Optimierung der Cloud-Migration, insbesondere im Hinblick auf branchenspezifische Anforderungen und Datenschutz. Eine tiefgehende Analyse der Wirtschaftlichkeit und langfristigen Stabilität von Cloud-Lösungen kann wertvolle Erkenntnisse liefern. Darüber hinaus ist eine Untersuchung der ökologischen Auswirkungen von Cloud-Technologien im Vergleich zu klassischen Serverlösungen ein wichtiger Beitrag zur Integration von Nachhaltigkeitsaspekten in IT-Strategien sein.

Glossar

5G

Die fünfte Generation des Mobilfunkstandards mit höheren Datenraten, geringerer Latenz und größerer Netzkapazität als frühere Generationen.

ADDS

(Active Directory Domain Services)

Ein Microsoft-Dienst zur Verwaltung von Netzwerken, Benutzern und Ressourcen in einer Windows-Domänenumgebung.

ASP

(Application Service Provider)

Ein Anbieter, der Softwareanwendungen und zugehörige Dienstleistungen über das Internet bereitstellt.

Bit/s

(Bit pro Sekunde)

Einheit für die Datenübertragungsrate, die angibt, wie viele Bits pro Sekunde übertragen werden können.

Cloud

Ein Netzwerk von Servern, die über das Internet bereitgestellte Speicher-, Rechen- und Softwaredienste ermöglichen.

DNS

(Domain Name System)

Ein System zur Übersetzung von menschenlesbaren Domainnamen (z. B. www.example.com) in IP-Adressen.

DSGVO

(Datenschutz-Grundverordnung)

Eine EU-Verordnung zum Schutz personenbezogener Daten und zur Regelung der Datenverarbeitung durch Unternehmen und Behörden.

Gbit/s

Siehe Bit/s.

HOST

Ein Computer oder Server, der in einem Netzwerk Ressourcen oder Dienste bereitstellt.

IaaS

(Infrastructure as a Service)

Ein Cloud-Computing-Dienstmodell, bei dem IT-Infrastruktur wie Rechenleistung, Speicher und Netzwerke als Service bereitgestellt werden.

IAM (Identity and Access Management)

Ein System zur Verwaltung von Benutzeridentitäten und Zugriffsrechten in einer IT-

Umgebung. IAM hilft Unternehmen, sicherzustellen, dass nur autorisierte Personen auf bestimmte Daten oder Systeme zugreifen können.

IPsec

(Internet Protocol Security)

Ein Protokoll zur Verschlüsselung und sicheren Übertragung von Daten über IP-Netzwerke.

ISP

(Internet Service Provider)

Ein Anbieter, der den Zugang zum Internet bereitstellt.

LDAP

(Lightweight Directory Access Protocol)

Ein Protokoll zur Abfrage und Verwaltung von Informationen in einem Verzeichnisdienst.

MFA

(Multi-Factor Authentication)

Eine Methode der Identitätsüberprüfung, bei der mindestens zwei unterschiedliche Faktoren (z. B. Passwort + SMS-Code oder Fingerabdruck) verwendet werden, um den Zugriff auf ein System sicherer zu machen.

Mbit/s

Siehe Bit/s.

NAS

(Network Attached Storage)

Ein netzwerkgebundener Speicher, der den Zugriff auf Dateien für mehrere Benutzer ermöglicht.

PaaS

(Platform as a Service)

Ein Cloud-Dienstmodell, das eine Entwicklungs- und Laufzeitumgebung für Anwendungen bereitstellt.

RBAC

(Role-Based Access Control)

Ein Berechtigungsmodell, bei dem der Zugriff auf Systeme oder Daten auf Basis von Benutzerrollen gewährt wird.

RFC

(Request for Comments)

Eine Reihe technischer und organisatorischer Dokumente, die Internetstandards und Protokolle beschreiben.

RPO

(Recovery Point Objective)

Der maximal tolerierbare Datenverlust in einem IT-System im Falle eines Ausfalls.

RTO

(Recovery Time Objective)

Die maximal akzeptable Zeitspanne für die Wiederherstellung eines IT-Systems nach einem Ausfall.

SaaS

(Software as a Service)

Ein Cloud-Dienstmodell, bei dem Softwareanwendungen über das Internet bereitgestellt werden.

USB

(Universal Serial Bus)

Ein Standard für die Verbindung und Kommunikation zwischen Computern und Peripheriegeräten.

VPN

(Virtual Private Network)

Eine sichere, verschlüsselte Verbindung über das Internet, die eine geschützte Kommunikation ermöglicht.

Zero Trust

Ein Sicherheitskonzept, das davon ausgeht, dass kein Benutzer oder Gerät automatisch als vertrauenswürdig gilt – unabhängig davon, ob sie sich innerhalb oder außerhalb des Netzwerks befinden. Jeder Zugriff muss kontinuierlich überprüft und validiert werden.

Literaturverzeichnis

- Abu-Dabaseh, Farah, und Esraa Alshammari. „Automated Penetration Testing : An Overview“. *Computer Science & Information Technology*, 2018. <https://doi.org/10.5121/csit.2018.80610>.
- Addis, Maria, und Maria Kutar. „The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness“. *UK Academy for Information Systems Conference Proceedings 2018*, 20. März 2018. <https://aisel.aisnet.org/ukais2018/29>.
- Ahmed, Mohamed, Sakshyam Panda, Christos Xenakis, und Emmanouil Panaousis. „MITRE ATT&CK-driven Cyber Risk Assessment“. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–10. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. <https://doi.org/10.1145/3538969.3544420>.
- Al-Sabaawi, Aiman, und Thamer A. Alrowidhan. „Detecting Network Security Vulnerabilities and Proactive Strategies to Mitigate Potential Threats“. arXiv, 22. Dezember 2022. <https://doi.org/10.48550/arXiv.2212.11449>.
- Alvarenga, Gui. „What Is a Cloud Workload Protection Platform? | CrowdStrike“. CrowdStrike.com, 15. Mai 2024. <https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-workload-protection-platform-cwpp/>.
- Arhinful, Clement, und Richard Essah. „Investigating Cloud Computing Security Measures and Risks“. *International Journal of Research Publication and Reviews*, Nr. 5 (Februar 2024): 1642–46.
- Attaran, Mohsen, und Jeremy Woods. „Cloud computing technology: improving small business performance using the Internet“. *Journal of Small Business & Entrepreneurship* 31, Nr. 6 (2. November 2019): 495–519. <https://doi.org/10.1080/08276331.2018.1466850>.
- Azodi, Amir, David Jaeger, Feng Cheng, und Christoph Meinel. „A New Approach to Building a Multi-tier Direct Access Knowledgebase for IDS/SIEM Systems“. In *2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing*, 118–23, 2013. <https://doi.org/10.1109/DASC.2013.48>.
- Baginda, Yorisan P., Achmad Affandi, und Istas Pratomo. „Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE)“. In *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 418–22, 2018. <https://doi.org/10.1109/ICITEED.2018.8534758>.
- Barati, Masoud, und Omer Rana. „Tracking GDPR Compliance in Cloud-Based Service Delivery“. *IEEE Transactions on Services Computing* 15, Nr. 3 (Mai 2022): 1498–1511. <https://doi.org/10.1109/TSC.2020.2999559>.
- Becker, Regina, Adrian Thorogood, Jasper Bovenberg, Colin Mitchell, und Alison Hall. „Applying GDPR roles and responsibilities to scientific data sharing“. *International Data Privacy Law* 12, Nr. 3 (1. August 2022): 207–19. <https://doi.org/10.1093/idpl/ipac011>.

- BMDW. „Small and Medium Enterprises in Austria – Facts and Figures“. Bundesministerium für Arbeit und Wirtschaft. Zugegriffen 30. Dezember 2024. <https://www.bmaw.gv.at/en/Topics/Business-Location/Small-and-medium-sized-Enterprises-SMEs/SME-in-Austria-facts-and-figures.html>.
- Bradley, Adrian. „The Key Cloud Trends in 2023 – and What They Mean for 2024 - KPMG UK“. KPMG, 29. Oktober 2024. <https://kpmg.com/uk/en/home/insights/2023/12/key-cloud-trends-in-2023.html>.
- Brataas, Grunnar, Nikolas Herbst, Simon Ivansek, und Jure Polutnik. „Scalability Analysis of Cloud Software Services“. In *2017 IEEE International Conference on Autonomous Computing (ICAC)*, 285–92, 2017. <https://doi.org/10.1109/ICAC.2017.34>.
- „Breitbandstrategie 2030“. Zugegriffen 2. Januar 2025. https://data.breitbandbuerogv.at/PUB_Breitbandstrategie-2030.pdf.
- Chalker, Alan, Curtis W. Hillegas, Alan Sill, Sharon Broude Geva, und Craig A. Stewart. „Cloud and on-premises data center usage, expenditures, and approaches to return on investment: A survey of academic research computing organizations“. In *Practice and Experience in Advanced Research Computing 2020: Catch the Wave*, 26–33. PEARC '20. New York, NY, USA: Association for Computing Machinery, 2020. <https://doi.org/10.1145/3311790.3396642>.
- „Client-Server“. Seite. Zugegriffen 30. Dezember 2024. https://www.e-teaching.org/technik/vernetzung/architektur/client-server/index_html.
- „Der richtige InternetZugang für Ihr Unternehmen“. Zugegriffen 2. Januar 2025. https://cdn2.hubspot.net/hubfs/344164/2016_DE_3forfree/Interactive_broadband_guide_DE.pdf.
- Dhiman, Poonam, Neha Saini, Yonis Gulzar, Sherzod Turaev, Amandeep Kaur, Khair Ul Nisa, und Yasir Hamid. „A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model“. *Sensors* 24, Nr. 4 (Januar 2024): 1328. <https://doi.org/10.3390/s24041328>.
- „Ethernet Cables Explained: Choosing The Right RJ45 Standard | Next7 IT“, 22. März 2024. <https://www.next7it.com/insights/ethernet-cables-explained-choosing-the-right-rj45-standard/>.
- Etro, Federico. „The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe. An Application of the Endogenous Market Structures Approach to a GPT Innovation“. *Review of Business and Economic Literature* LIV, Nr. 2 (2009): 179–208.
- Fahmideh, Mahdi, Farhad Daneshgar, Ghassan Beydoun, und Fethi Rabhi. „Challenges in migrating legacy software systems to the cloud an empirical study“. arXiv, 17. April 2020. <https://doi.org/10.48550/arXiv.2004.10724>.
- Fallara, P. „Disaster recovery planning“. *IEEE Potentials* 23, Nr. 5 (Dezember 2004): 42–44. <https://doi.org/10.1109/MP.2004.1301248>.
- Fechner, Jan. „Einsatz Künstlicher Intelligenz (KI/AI) in der Informationssicherheit“. *NESEC Blog* (blog), 14. April 2024. <https://blog.nesec.de/ki/einsatz-kuenstlicher-intelligenz-ki-ai-in-der-cybersicherheit/>.

- Fisher, Cameron. „Cloud versus On-Premise Computing“. *American Journal of Industrial and Business Management* 8, Nr. 9 (4. September 2018): 1991–2006. <https://doi.org/10.4236/ajibm.2018.89133>.
- Forrester. „Predictions 2024: Cloud Computing“. Zugegriffen 2. Januar 2025. <https://www.forrester.com/webinar/predictions-2024-cloud-computing/WEB40235>.
- Gaianu, Mihail. „On Premise Data Center vs CLOUD“. In *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 1068–71, 2023. <https://doi.org/10.1109/CSCI62032.2023.00176>.
- „Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600bln in 2023“. Zugegriffen 2. Januar 2025. <https://www.zawya.com/en/press-release/research-and-studies/gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600bln-in-2023-b3fygmz3>.
- General Data Protection Regulation (GDPR). „Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority“. Zugegriffen 3. Februar 2025. <https://gdpr-info.eu/art-33-gdpr/>.
- GitHub-Name. „Windows Server 2012 R2 - Microsoft Lifecycle“. Zugegriffen 30. Dezember 2024. <https://learn.microsoft.com/de-de/lifecycle/products/windows-server-2012-r2>.
- „Google Docs | History, Features, & Facts | Britannica“, 13. Dezember 2024. <https://www.britannica.com/topic/Google-Docs>.
- Halbouni, Asmaa, Lee-Yeng Ong, und Meng-Chew Leow. „Wireless Security Protocols WPA3: A Systematic Literature Review“. *IEEE Access* 11 (1. Januar 2023): 112438–50. <https://doi.org/10.1109/ACCESS.2023.3322931>.
- Hawkins, Steve M., David C. Yen, und David C. Chou. „Disaster recovery planning: a strategy for data security“. *Information Management & Computer Security* 8, Nr. 5 (1. Januar 2000): 222–30. <https://doi.org/10.1108/09685220010353150>.
- Indu, I., P. M. Rubesh Anand, und Vidhyacharan Bhaskar. „Identity and access management in cloud environment: Mechanisms and challenges“. *Engineering Science and Technology, an International Journal* 21, Nr. 4 (1. August 2018): 574–88. <https://doi.org/10.1016/j.jestch.2018.05.010>.
- Kersken, Sascha. *IT-Handbuch für Fachinformatiker: der Ausbildungsbegleiter*. 7., aktualisierte und erweiterte Auflage 2015, 1. korrigierter Nachdruck 2016. Rheinwerk Computing. Bonn: Rheinwerk Verlag GmbH, 2016.
- Khoshkholghi, Mohammad Ali, Abdullah Azizol, Latip Rohaya, Subramaniam Shamala, und Othman Mohamed. „Disaster Recovery in Cloud Computing: A Survey“. *Computer and Information Science* 7, Nr. 4 (September 2014): 39. <https://doi.org/10.5539/cis.v7n4p39>.
- Kozlovsky, M. „Cloud Security Monitoring and Vulnerability Management“. In *Critical Infrastructure Protection Research: Results of the First Critical Infrastructure Protection Research Project in Hungary*, herausgegeben von László Náday und József Padányi, 123–39. Cham: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-28091-2_11.

- Kraemer, Sara, Pascale Carayon, und Ruth Duggan. „Red Team Performance for Improved Computer Security“. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 48, Nr. 14 (1. September 2004): 1605–9. <https://doi.org/10.1177/154193120404801410>.
- Krisper, Michael. „Problems with Risk Matrices Using Ordinal Scales“. arXiv, 7. März 2021. <https://doi.org/10.48550/arXiv.2103.05440>.
- Li, He, Lu Yu, und Wu He. „The Impact of GDPR on Global Technology Development“. *Journal of Global Information Technology Management* 22, Nr. 1 (2. Januar 2019): 1–6. <https://doi.org/10.1080/1097198X.2019.1569186>.
- Liu, Qing, und Qiuping Liu. „A Study on Topology in Computer Network“. In *2014 7th International Conference on Intelligent Computation Technology and Automation*, 45–48, 2014. <https://doi.org/10.1109/ICICTA.2014.18>.
- Lynn, Theo. „Dear Cloud, I Think We Have Trust Issues: Cloud Computing Contracts and Trust“. In *Data Privacy and Trust in Cloud Computing: Building Trust in the Cloud through Assurance and Accountability*, herausgegeben von Theo Lynn, John G. Mooney, Lisa van der Werff, und Grace Fox, 21–42. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-54660-1_2.
- Meyer, Lawrence E., und E. Billionniere. „Upskilling to Meet Cloud Talent Needs“. *2021 ASEE Virtual Annual Conference*, Juli 2021. <https://par.nsf.gov/biblio/10288742-upskilling-meet-cloud-talent-needs>.
- Mhlongo, Noluthando Zamanjomane, Favour Oluwadamilare Usman, Olubusola Odeyemi, Chinedu Ugochukwu Ike, Oluwafunmi Adijat Elufioye, Andrew Ifesinachi Daraojimba, Noluthando Zamanjomane Mhlongo, u. a. „Reviewing the Impact of Cloud Computing on Small and Medium Enterprises in Africa“. *International Journal of Science and Research Archive* 11, Nr. 1 (2024): 1444–51. <https://doi.org/10.30574/ijrsra.2024.11.1.0236>.
- Mohammed, Kabiru Hamza, Abubakar Hassan, und Danlami Yusuf Mohammed. „Identity and Access Management System: A Web-Based Approach for an Enterprise“, 2018. <http://oer.udusok.edu.ng:8080/xmlui/handle/123456789/837>.
- Mohammed, Zareef. „Data Breach Recovery Areas: An Exploration of Organization’s Recovery Strategies for Surviving Data Breaches“. *Organizational Cybersecurity Journal: Practice, Process and People* 2, Nr. 1 (9. November 2021): 41–59. <https://doi.org/10.1108/OCJ-05-2021-0014>.
- Mohapatra, Sanjay, und Laxmikant Lokhande. *Cloud Computing and ROI: A New Framework for IT Strategy*. Management for Professionals. Cham: Springer International Publishing, 2014. <https://doi.org/10.1007/978-3-319-08663-7>.
- Moore, Tristan L, Samule Conlon, Anushka Hewarathna, und Thivanka P B M Disanayaka. „Encryption Methods and Key Management Services for Secure Cloud Computing: A Review“. In *ResearchGate*, 2023. https://www.researchgate.net/publication/369777264_Encryption_Methods_and_Key_Management_Services_for_Secure_Cloud_Computing_A_Review.
- Papadaki, Maria, und Steven Furnell. „IDS or IPS: what is best?“ *Network Security* 2004, Nr. 7 (1. Juli 2004): 15–19. [https://doi.org/10.1016/S1353-4858\(04\)00106-0](https://doi.org/10.1016/S1353-4858(04)00106-0).

- Park, Juyeon, und Marilyn DeLong. „User Perceptions of Technology Adoption and Implementation: A Case Study of Footwear Production in a Global Market“. *Fashion Practice* 1, Nr. 1 (1. Mai 2009): 87–108. <https://doi.org/10.2752/175693809X418865>.
- Pattakou, Argyri, Vasiliki Diamantopoulou, Christos Kalloniatis, und Stefanos Gritzalis. „A Unified Framework for GDPR Compliance in Cloud Computing“. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–9. Vienna Austria: ACM, 2024. <https://doi.org/10.1145/3664476.3670918>.
- Perifanis, Nikolaos-Alexandros, und Fotis Kitsios. „Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review“. *Information* 14, Nr. 2 (Februar 2023): 85. <https://doi.org/10.3390/info14020085>.
- Pramod, N., Anil Kumar Muppalla, und K. G. Srinivasa. „Limitations and Challenges in Cloud-Based Applications Development“. In *Software Engineering Frameworks for the Cloud Computing Paradigm*, herausgegeben von Zaigham Mahmood und Saqib Saeed, 55–75. London: Springer, 2013. https://doi.org/10.1007/978-1-4471-5031-2_3.
- PricewaterhouseCoopers. „From Threat to Opportunity | PwC’s Global Risk Survey 2023“. PwC. Zugriffen 2. Januar 2025. <https://www.pwc.com/gx/en/issues/risk-regulation/global-risk-survey.html>.
- Qaqos, Noor N. A. J. E. B. „Opnet Based Performance Analysis and Comparison Among Different Physical Network Topologies“. *Academic Journal of Nawroz University (AJNU)*, 1. Januar 2018, 48–54. <https://doi.org/10.25007/ajnu.v7n3a199>.
- Qasmi, Wasiq Noor Ahmad, Taimur Siddiqui, Muhammad Karam Shehzad, Adnan Iqbal, und Muhammad Saqib Ilyas. „A comparative study of failover schemes for IaaS recovery“. In *2018 International Conference on Information Networking (ICOIN)*, 25–30, 2018. <https://doi.org/10.1109/ICOIN.2018.8343078>.
- Rajesh, Siddharth Choudhary. „High Availability Strategies in Distributed Systems: A Practical Guide“. *International Journal of Research in All Subjects in Multi Languages*, Nr. 13 (18. Januar 2025): 110–30.
- Ranganathan, Chitra Sabapathy, und Rajeshkumar Sampathrajan. „Cloud Migration Meets Targeted Deadlines“. In *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 672–76, 2023. <https://doi.org/10.1109/ICESC57686.2023.10193104>.
- Sahut, Jean Michel, und Raphael Lissillour. „The Adoption of Remote Work Platforms after the Covid-19 Lockdown: New Approach, New Evidence“. *Journal of Business Research* 154 (1. Januar 2023): 113345. <https://doi.org/10.1016/j.jbusres.2022.113345>.
- Salesforce. „Salesforce Official Web Site“. Zugriffen 2. Januar 2025. <https://www.salesforce.com/de/company/our-story/>.
- Schlehahn, Eva, und Rigo Wenning. „GDPR Transparency Requirements and Data Privacy Vocabularies“. In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7*,

- 11.6/SIG 9.2.2 *International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, herausgegeben von Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner, und Stephan Krenn, 95–113. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-16744-8_7.
- Schmitz, Peter, und Stefan Luber. „Was ist ein Domänencontroller?“ *Security-Insider*, 10. Februar 2021. <https://www.security-insider.de/was-ist-ein-domaenencontroller-a-1021654/>.
- Statista. „Betriebssysteme - Marktanteile weltweit 2024“. Zugegriffen 30. Dezember 2024. <https://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/>.
- Team, Editorial. „Fault Tolerance“. *Network Encyclopedia*, 11. September 2019. <https://networkencyclopedia.com/fault-tolerance/>.
- „Topologien – IT-Datenbank.com“, 29. August 2020. <https://it-datenbank.com/topologien/>.
- Van Landuyt, Dimitri, und Wouter Joosen. „A Descriptive Study of Assumptions in STRIDE Security Threat Modeling“. *Software and Systems Modeling* 21, Nr. 6 (1. Dezember 2022): 2311–28. <https://doi.org/10.1007/s10270-021-00941-7>.
- Wang, Zhixiao, Wen Yao Yan, und Wendong Wang. „Revisiting Cloud Migration: Strategies and Methods“. *Journal of Physics: Conference Series* 1575, Nr. 1 (Juni 2020): 012232. <https://doi.org/10.1088/1742-6596/1575/1/012232>.
- „Windows Server 2022 Editionsunterschiede – Thomas-Krenn-Wiki“. Zugegriffen 2. Januar 2025. https://www.thomas-krenn.com/de/wiki/Windows_Server_2022_Editionsunterschiede.
- Wu, Zi Qiang, und Hui Li. „Analysis of Data Backup and Recovery System“. *Applied Mechanics and Materials* 631–632 (2014). <https://doi.org/10.4028/www.scientific.net/amm.631-632.1207>.
- Zaguir, Nemer Alberto, Guilherme Henrique de Magalhães, und Mauro de Mesquita Spinola. „Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions“. *IEEE Access* 12 (2024): 81608–30. <https://doi.org/10.1109/ACCESS.2024.3406724>.

Abbildungsverzeichnis

Abbildung 1: Server-Client Modell	5
Abbildung 2: Netzwerktopologien	7
Abbildung 3: Schematische Darstellung eines einfachen Firmennetzwerkes.....	9
Abbildung 4: Netzwurkkabel	10

Tabellenverzeichnis

Tabelle 1: Vergleich Edition/Lizenz Microsoft Windows Server 2022	11
Tabelle 2: Vergleich der Vor- und Nachteile von lokalen Serverumgebungen und webgehosteten Services	21
Tabelle 3: Typische Bandbreitenanforderungen nach Nutzungsszenario	26
Tabelle 4: Herausforderungen und empfohlene Lösungen bei der Migration verschiedener Datenarten	28
Tabelle 5: Typische Kompatibilitätsprobleme und Lösungsansätze	29
Tabelle 6: Vergleich lokaler und Cloud-basierter Authentifizierungssysteme	30
Tabelle 7: Vergleich der Skalierbarkeit und Wartung zwischen lokalen Servern und webgehosteten	31
Tabelle 8: Vergleich der langfristigen Kosten zwischen lokalen Servern und webgehosteten Services	32
Tabelle 9: ROI-Vergleich zwischen lokalen Servern und webgehosteten Services über verschiedene Zeiträume	35
Tabelle 10: Phasen und Zeitrahmen der Migration zu webgehosteten Services	37
Tabelle 11: Schulungsplan für die Einführung webgehosteter Services	38
Tabelle 12: Vergleich der Datenschutz- und Sicherheitsanforderungen zwischen lokalen Servern und webgehosteten Services	41
Tabelle 13: Vergleich der Sicherheitsmaßnahmen zwischen traditioneller IT und Cloud-Sicherheit	45
Tabelle 14: Risikobewertung und empfohlene Gegenmaßnahmen für Cloud-Sicherheit	46
Tabelle 15: Vergleich von Schutzmaßnahmen zwischen traditioneller IT-Sicherheit und Cloud-Sicherheit	47
Tabelle 16: Vergleich der Backup-Methoden hinsichtlich Speicherbedarfes, Sicherungszeit und Wiederherstellungszeit	49
Tabelle 17: Vergleich von Redundanzstrategien für Notfallwiederherstellung	51
Tabelle 18: Bewertung der Notfallwiederherstellungs- und Redundanzstrategie	52