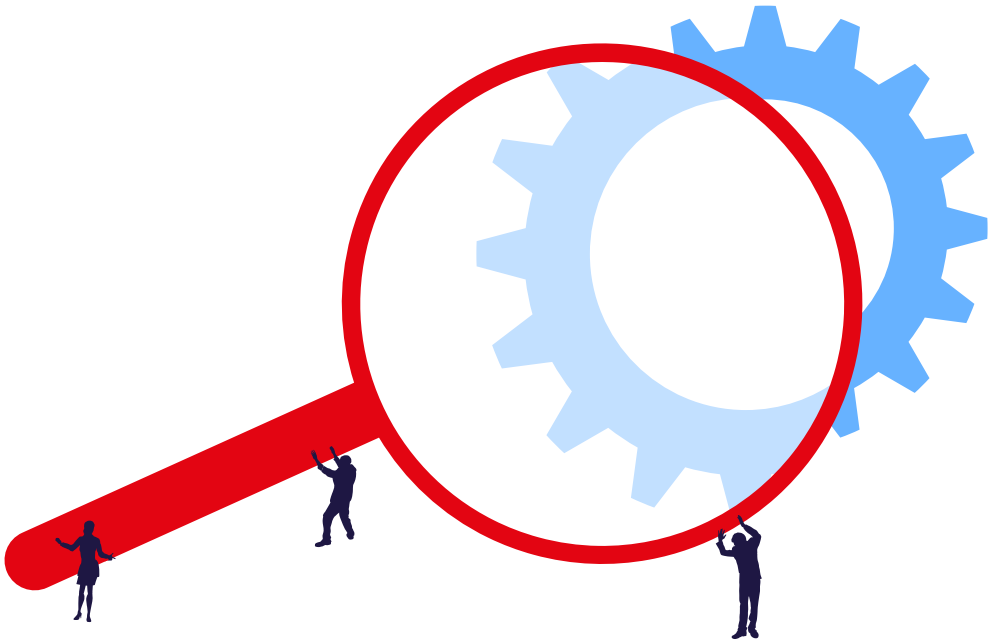
Digitale Verwaltung Schweiz
Administration numérique suisse
Amministrazione digitale Svizzera

Second Source

Studie im Auftrag der Arbeitsgruppe
«Cloud Governance und Workplace»
der Digitalen Verwaltung Schweiz



April 2025

ELCA ADVISORY

Second Source – Studie

Klassifizierung	nicht klassifiziert
Status	genehmigt zur Nutzung
Projektleitung	Olaf Sparka, Erich Hofer
Version	1.0
Datum	23. April 2025
Auftraggeber	Arbeitsgruppe «Cloud Governance und Workplace» der DVS
Autor/Autoren	ELCA Advisory

ELCA Informatik AG
Flurstrasse 62 | 8048 Zürich
Tel. +41 (0)44 456 32 11 | Fax +41 (0)44 456 32 00
www.elca.ch
Pully | Zürich | Genève | Bern | Basel | Rapperswil-Jona | Italy | Spain | Mauritius | Vietnam

Änderungsverzeichnis

Version	Datum	Änderung	Autor
0.1	November 2024	Erster Entwurf der Kapitel 1 bis 5	Luca Schädler, Nadine Tschichold
0.2	Dezember 2024 – 8.1.2025	Einarbeiten der Review-Kommentare von Olaf Sparka, Ergänzungen zu Kap. 5, Aufnahme Kap. «Zusammenfassung» sowie Kap. 6 bis 10	Luca Schädler, Nadine Tschichold
0.3	9.– 30.1.2025	Einarbeiten der Review-Kommentare zu Kapitel 6 bis 10 gemäss Review-Meetings vom 9.12.2025 und vom 27.1.25 mit der Projektleitung	Luca Schädler, Nadine Tschichold, Projektleitung DVS
0.4	30.1.2025 – 14.02.2025	Einarbeiten der Review-Kommentare der Arbeitsgruppe und Interview-Partnern, deren Auswertung mit der Projektleitung.	Luca Schädler, Nadine Tschichold, Projektleitung DVS
0.5	17.02.2025	Einarbeiten der Ergebnisse der Review-Besprechung mit der Projektleitung vom 14.2.2025	Luca Schädler, Nadine Tschichold, Projektleitung DVS
0.6	21.02.2025	Sprachliche Korrekturen, Versand zu Review seitens operative Leitung DVS	Luca Schädler, Nadine Tschichold
1.0	23.04.2025	Finale Version	Nadine Tschichold

Vorwort

Im Zuge der fortschreitenden Digitalisierung der Verwaltung müssen sich Behörden zunehmend mit konkreten Fragen rund um Cloud-Dienste und deren sicheren Einsatz befassen. Microsoft 365 steht dabei häufig im Zentrum der Betrachtung: Die Plattform ist weit verbreitet und bietet vielfältige Möglichkeiten zur Effizienzsteigerung. Gleichzeitig birgt der Einsatz solcher Services neue Risiken, die – wie bei jeder Nutzung von IT-Mitteln – sorgfältig analysiert und gemanagt werden müssen.

Diese Studie der Arbeitsgruppe «Cloud-Governance und Workplace» greift drei zentrale Fragen auf, mit denen sich Verwaltungen beim produktiven Einsatz von Microsoft-Diensten in der Cloud konfrontiert sehen.

Das Ziel der Studie ist es, den aktuellen Zustand – die IST-Situation – neutral und sachlich darzustellen und transparent aufzuzeigen, wo gezielte risikominimierende Massnahmen realisiert werden können. Gleichzeitig wird dargelegt, in welchen Bereichen umfassendere oder koordinierte Massnahmen erforderlich sein könnten.

Die Studie verzichtet bewusst auf eine Bewertung technischer Lösungen oder eine vertiefte Machbarkeitsanalyse. Die dargestellten Erkenntnisse basieren auf den Informationen und Angaben einzelner Lieferanten sowie auf eine Studie der Berner Fachhochschule und das Wissen der Autoren der vorliegenden Studie. Diese Erkenntnisse sollen eine objektive, fundierte Grundlage für weiterführende Aktivitäten bieten.

Ergeben sich aus der im Rahmen der Verbreitung dieser Studie durchgeführten Kurz-Umfrage zusätzliche Handlungsfelder, wird die Arbeitsgruppe prüfen, ob sich diese für ein Folgeprojekt eignen.

Zusammenfassung

Die vorliegende Studie wurde von ELCA Advisory im Auftrag der Arbeitsgruppe «Cloud Governance und Workplace» (DVS) erarbeitet und beleuchtet zentrale Fragen zu den Chancen und Herausforderungen rund um die Abhängigkeit der öffentlichen Verwaltung von proprietärer Microsoft-Software und software-basierten Services, insbesondere im Bereich der Büroautomation. Grundlage der Analyse waren Interviews mit Vertretern öffentlicher Institutionen sowie eine Marktanalyse mittels «Request for Information» (RFI) bei Firmen mit Firmensitz in der Schweiz oder in der EU, um die Einhaltung spezifischer rechtlicher Rahmenbedingungen und Datenschutzanforderungen sicherzustellen. Die Auswertungen der Marktanalyse und deren Fazit, inklusive der Formulierungen für mögliche nächste Schritte aus technischer Sicht (z.B. in Kapitel 9) wurden in enger Zusammenarbeit der DVS-Arbeitsgruppe «Cloud Governance und Workplace» und ELCA Advisory formuliert. Die übrigen Handlungsempfehlungen wurden von der DVS-Arbeitsgruppe erarbeitet und in die Studie integriert.

Die allgemeinen Erkenntnisse zu Souveränitäts-Überlegungen sind grundsätzlich auf weitere Anbieter und Services übertragbar. Jedoch beschränkt sich die vorliegende Studie auf die M365 Services von Microsoft, weil diese ein aktuelles Thema in den öffentlichen Institutionen der Schweiz sind.

Erkenntnisse

1. **Vielfalt potenzieller Alternativen**
   Der Markt bietet vielversprechende Produktalternativen im Bereich der Büroautomation. Anbieter wie VNCLagoon, InfoManiak, EGroupware sowie das Zentrum Digitale Souveränität (ZenDiS), das im Besitz öffentlicher Institutionen ist, arbeiten an Lösungen mit dem Ziel, die Funktionsvielfalt von Microsoft zu erreichen. Vielversprechende Pilotprojekte, wie jenes der Bundeskanzlei in der Schweiz und Initiativen auf Landesebene in Deutschland (z. B. Schleswig-Holstein), zeigen den innovativen Ansatz und die Entschlossenheit, die digitale Souveränität in diesem Bereich zu stärken. Diese Projekte bieten eine solide Basis für zukünftige Entwicklungen und geben wertvolle Einblicke in mögliche Alternativen.
2. **Stärkung der Resilienz durch IT-SCM**
   Diese Studie zeigt, dass es in gewissen Bereichen praktikable Ansätze gibt, um die IT-Resilienz zu verbessern. Besonders im Bereich Audio-/Video-Conferencing und E-Mail-Services existieren Optionen, die bei Bedarf rasch einsatzbereit sein können, allerdings mit Einbussen an Funktionsumfang. Parallelbetrieb und vorausschauende Planung können die Handlungsfähigkeit im Ernstfall erheblich erhöhen. Diese sind zwar mit Mehraufwand und Kosten verbunden, jedoch stärkt die Implementierung solcher Lösungen die Souveränität und stellt sicher, dass essentielle Funktionen auch in Störungsszenarien gewährleistet sind. Der Umfang der Massnahmen und der Umsetzung ist abhängig vom Risikomanagement der jeweiligen Institutionen, deshalb muss der Entscheid von ihnen getroffen werden. Bezüglich des weiteren Ausbaus und der Optimierung der Massnahmen wäre ein Austausch oder sogar eine koordinierte Zusammenarbeit zwischen den Institutionen zielführend.
3. **Strategischer Übergang und Migration**
   Möchte eine Institution von Microsoft-Services hin zu Alternativen übergehen erfordert

dies eine strategische und politische Entscheidung, die Bereitschaft zumindest kurzfristig höhere Kosten zu tragen sowie eine langfristig ausgerichtete Planung. Die bisherigen Pilotprojekte zeigen: Eine gute Chance für die Machbarkeit ist, dass Institutionen gemeinsame Ziele verfolgen und die Aktivitäten von zentralen Organisationen wie eOperations oder DVS koordiniert und gesteuert werden könnten. Auch technische Herausforderungen, wie die Migration von Fachanwendungen, sollten durch koordinierte Ansätze (z.B. Verhandlungen mit Anbietern von Fachanwendungen, die in mehreren Kantonen eingesetzt werden) und gezielte Schulungen der Benutzer angegangen werden. Zudem sollten Interoperabilität und offene Standards bereits bei der Beschaffung berücksichtigt werden.

Die aktuell verfügbaren und in Entwicklung befindlichen alternativen Services erfordern Kompromisse und Anpassungen an die bestehende IT-Services und Fachanwendungen, was den Wechsel besonders anspruchsvoll macht. Deren Bereitstellung sowie ein Umstieg ist ressourcen- und zeitintensiv. Mit der Integration neuer Services von Microsoft (z.B. Copilot, Power-Platform) wird ein Umstieg immer aufwendiger. Ein isoliertes Vorgehen einzelner öffentlicher Institutionen ist ressourcenintensiv und birgt erhebliche Risiken. Nicht zu unterschätzen sind zudem mögliche Widerstände von Endnutzenden gegenüber alternativen Services, welche die «gelernten» und gut integrierten Applikationen ablösen könnten.

Positive Entwicklungen und Perspektiven

Diese Studie zeigt, dass es bereits starke Bestrebungen gibt, die digitale Souveränität der öffentlichen Verwaltung zu fördern und dass zahlreiche Institutionen an innovativen Lösungen dafür arbeiten. Initiativen wie die Swiss Government Cloud (SGC) oder die zentralisierte Planung durch öffentliche Organisationen zeigen den Willen und die Fähigkeit, die Abhängigkeit von Einzellösungen grundsätzlich zu reduzieren. Dabei wird grosser Wert daraufgelegt, flexible und skalierbare Lösungen zu entwickeln, die den Anforderungen unterschiedlicher Institutionen gerecht werden.

Fazit

Die **Stärkung der digitalen Souveränität** ist kein einfacher Prozess. Die vorliegenden Ansätze und Bestrebungen verdeutlichen, dass ein solcher Wandel nicht nur von vielen Institutionen gewünscht, sondern prinzipiell auch realisierbar ist. Der Preis für die Stärkung der digitalen Souveränität ist allerdings neben höheren betrieblichen Kosten auch eine ansteigende operative Komplexität. Deshalb sind eine enge Zusammenarbeit zwischen Bund, Kantonen und Gemeinden sowie eine zentrale Koordination notwendig, um Lösungen zu schaffen, die nicht nur effektiv, sondern auch nachhaltig und skalierbar sind. Dabei ist es besonders wichtig, dass der Fokus darauf liegt, neue Abhängigkeiten zu vermeiden und langfristige Perspektiven zu schaffen.

Auf Basis der Studie können vier zentrale Handlungsfelder hergeleitet werden, die bei der Transformation und Stärkung der digitalen Souveränität berücksichtigt werden müssen:

- Erstens geht es um den technischen Ersatz bestehender Anwendungen, deren Betrieb sowie die nahtlose Integration in die bestehende IT-Infrastruktur. Dies erfordert nicht nur technische Lösungen, sondern auch ein tiefes Verständnis der Wechselwirkungen zwischen verschiedensten Services und die Integration in Fachanwendungen, um Ausfälle oder Funktionsverluste zu vermeiden.

- Zweitens muss bei Weiterentwicklungen von Microsoft-Services geprüft werden, inwieweit diese eingeführt werden sollen, da gegebenenfalls bestehende Konzepte von Alternativlösungen entsprechend erweitert werden müssen.
- Drittens müssen dafür gemeinsame Standards definiert werden (z.B. Office-Format), die eine einheitliche und interoperable Entwicklung fördern. Dies ist entscheidend, um zu verhindern, dass verschiedene Akteure und Nutzer in nicht kompatiblen Richtungen arbeiten, was langfristig zu hoher Komplexität und erhöhten Kosten führen würde. Gemeinsame Standards ermöglichen zudem eine koordinierte und effiziente Zusammenarbeit.
- Viertens stellt sich die Betreiberfrage, die strategisch und langfristig geklärt werden muss. Ein Wechsel von einem privatwirtschaftlichen Anbieter zu einem anderen löst das Grundproblem der Abhängigkeit nicht. Im Falle von Open Source Software bleibt zudem offen, wie ein zukunftsfähiges Betriebsmodell aussehen könnte, das nicht nur die Funktionalität, sondern auch die notwendige Sicherheit und Stabilität gewährleistet. Hier bedarf es innovativer Ansätze, um Betrieb und Weiterentwicklung nachhaltig und sicher zu gestalten.

Diese Handlungsfelder unterstreichen die Komplexität der Herausforderungen, bieten jedoch auch klare Ansatzpunkte für eine strategische und koordinierte Herangehensweise.

Die Erkenntnisse dieser Studie verdeutlichen, dass einzelne Verwaltungen kaum in der Lage sein werden, allein tragfähige Lösungen für die beschriebenen Herausforderungen zu entwickeln. Die Komplexität der technischen, organisatorischen und rechtlichen Anforderungen erfordert eine enge Zusammenarbeit. Ein Zusammenschluss der Akteure – idealerweise auf nationaler und sogar überstaatlicher Ebene, beispielsweise in Kooperation mit der EU – ist entscheidend, um Synergien zu schaffen, Standards zu entwickeln und Ressourcen effizient zu nutzen. Nur durch eine koordinierte, übergreifende Herangehensweise können langfristig nachhaltige und souveräne Lösungen realisiert werden.

Eine **Notfalllösung** ohne jegliche Datenvorhaltung, Migration und Integration könnte jedoch für die meisten untersuchten Services relativ einfach aufgebaut und betrieben werden (auch im Standby Modus). Den Nutzen einer solchen Umgebung, welche NUR eine minimale Funktionalität sicherstellt, muss jede Organisation für sich beurteilen. Das könnte z.B. für eine kleinere spezialisierte Gruppe wie VIP, eine Notfallorganisation, einen Krisenstab, Kommunikationsverantwortliche, usw. sinnvoll sein, um in Notfallsituationen operativ- und mit gewissen Restriktionen weiterarbeiten zu können und dabei gleichzeitig die Zusatzaufwände in Grenzen zu halten.

Eine solche Notfalllösung wird jedoch hochgradig komplex und aufwendig, sobald Daten vorgehalten oder synchronisiert werden müssen. Für einen effektiven und effizienten Notfallbetrieb, der es breiten Mitarbeitergruppen ermöglicht, ihre Geschäftstätigkeit anhand der wichtigsten Geschäftsprozesse auch im Notfall weiterführen zu können, wäre dies jedoch vermutlich notwendig. Jede Organisation muss also im Rahmen des normalen Risikomanagements selbst herausfinden, welche Lösungen sie im Notfall im Sinne einer Rückversicherung braucht und welche Lösung sie sich leisten will und kann.

Abgrenzung

Diese Studie hatte den klaren Fokus, die aktuelle Situation der öffentlichen Verwaltung im Umgang mit proprietären Softwarelösungen und Services aufzuzeigen. Dabei wurde bewusst eine Perspektive auf hoher Flughöhe eingenommen, um ein umfassendes Bild der Ist-Situation zu zeichnen. Es ging nicht darum, technische Machbarkeiten oder Lösungen detailliert miteinander zu vergleichen oder spezifische Ursachen oder Alternativen vertieft zu analysieren. Vielmehr lag der Schwerpunkt darauf, Verwaltungen Ansätze für eine langfristige Strategie aufzuzeigen.

Inhaltsverzeichnis

1 Einleitung

Die öffentliche Verwaltung in der Schweiz ist sich der bestehenden Abhängigkeit von proprietärer Software, insbesondere von Microsoft-Services, bewusst. Diese betrifft Büroautomation-, Kollaborations- und Kommunikationslösungen wie MS-Office, SharePoint, Teams und Outlook bzw. Exchange. Mit wachsendem Bedarf an digitaler Souveränität steigt das Interesse an alternativen Softwarelösungen, die eine grössere Unabhängigkeit von einzelnen Firmen ermöglichen.

Die Arbeitsgruppe «Cloud Governance und Workplace» der Digitalen Verwaltung Schweiz (DVS) hat die vorliegende Studie beauftragt, mögliche Open Source Software (OSS) Alternativen zu den Microsoft-Services zu untersuchen. Das Ziel dieses Auftrags war zu prüfen, ob und welche Möglichkeiten existieren, die als echte, machbare Alternativen die Abhängigkeit der Verwaltung von Microsoft-Services reduzieren können. Es wird untersucht, welche OSS-Alternativen derzeit in Europa verfügbar sind, die als vollwertiger Ersatz zu Microsoft-Services dienen können. Dabei stehen zwei Szenarien im Vordergrund, zum einen für IT Service Continuity Management (IT-SCM) und zum anderen für den Ausstieg von Microsoft-Services, wobei dieser Ausstieg vollständig oder teilweise, d.h. nur für einzelne Microsoft-Services, erfolgen kann.

Die vorliegende Studie soll eine Orientierung bieten, inwieweit OSS-Lösungen, zum heutigen Zeitpunkt, die Anforderungen der öffentlichen Verwaltung erfüllen und einen Beitrag zur digitalen Souveränität der Schweiz leisten können. Die Verwaltungseinheiten in der Schweiz können die Ergebnisse dieser Studie als Grundlage verwenden, um eine eigene, belastbare Strategie zur schrittweisen Reduktion ihrer Abhängigkeit von Microsoft-Software und anderen proprietären Lösungen zu entwickeln. Gemäss Aufgabenstellung der Studie ist das übergeordnete Ziel der Verwaltungen, ihre Abhängigkeit von einzelnen privatwirtschaftlichen Unternehmen zu verringern und somit die digitale Souveränität zu stärken.

Begriffserklärung:

In dieser Studie wird der Begriff IT Service Continuity Management (IT-SCM) verwendet, um den Fokus auf die strategischen Massnahmen zur Sicherstellung der Verfügbarkeit von IT-Services im Falle von Störungen oder Ausfällen zu lenken.

- **Business Continuity Management (BCM)** ist die planerische Sicherstellung der Handlungsfähigkeit der Verwaltung auch in einem Notfall oder einer Krise . Im Fokus steht die Frage: Wie können wir unsere Aufgaben erledigen, egal was passiert? Beispiel: Was machen wir, wenn ein IT-Service ganz ausfällt, das Gebäude mit den Büroräumlichkeiten brennt, eine Pandemie ausbricht oder andere Risiken eintreten?
- **IT Service Continuity Management (IT-SCM)** ist ein Teil des BCM, aber speziell auf IT-Services bezogen. Hier geht es darum sicherzustellen, dass IT-Services (z. B. E-Mail, Telefonie) auch bei Störungen schnell wieder verfügbar sind. Die Frage hier ist: Wie stellen wir sicher, dass unsere IT funktioniert, auch wenn es Probleme gibt? Beispiel: Wie können wir einen ausgefallenen IT-Service vorübergehend mit einem anderen ersetzen?

Die **Annahme für die vorliegende Studie**, basierend auf den durchgeführten Interviews, ist, dass im Falle eines IT-SCM-Szenarios die Wiederverfügbarkeit der IT-Services innerhalb weniger Tage (etwa einer Woche) erfolgt. Die tatsächliche Dauer hängt jedoch von der jeweiligen Organisation, den betroffenen Services sowie dem zugrunde liegenden Risikomanagement ab.

2 Ziele und Umfang der Studie

Im Rahmen des Projekts «Second Source» sollten einige zentrale Fragen beantwortet werden, die jede Verwaltungseinheit im öffentlichen Sektor klären muss, wenn sie Microsoft Services (M365-Services, insbesondere Kommunikations- und Kollaborationsprodukte) in der Cloud nutzen möchte. Das Ziel dieser Studie ist es, diese Antworten zentral und allgemein gültig zu erarbeiten, so dass sie von allen Verwaltungseinheiten im öffentlichen Sektor (insbesondere Kantone und Gemeinden) übernommen und auf ihre spezifische Situation adaptiert werden können, idealerweise höchstens mit minimalen, eigenen Zusatzabklärungen. Der Fokus der Studie liegt dabei auf der Untersuchung der folgenden Fragen:

- Welche Open Source Alternativen zu Microsoft Services stehen heute zur Verfügung?
- Welche Möglichkeiten gibt es, Microsoft Services durch eine Alternative zu unterstützen, insbesondere im Hinblick auf ein IT-SCM? Welche Massnahmen können oder sollten bereits jetzt ergriffen werden, um im Ernstfall gut vorbereitet zu sein?
- Welche Schritte können oder sollten heute eingeleitet werden, um sich auf ein potenzielles Vertragsende vorzubereiten – sei es durch eine eigene Kündigung oder durch eine Kündigung seitens Microsoft?

Diese Fragestellungen wurden für die Microsoft-Services gemäss Abbildung 1 untersucht und beantwortet.

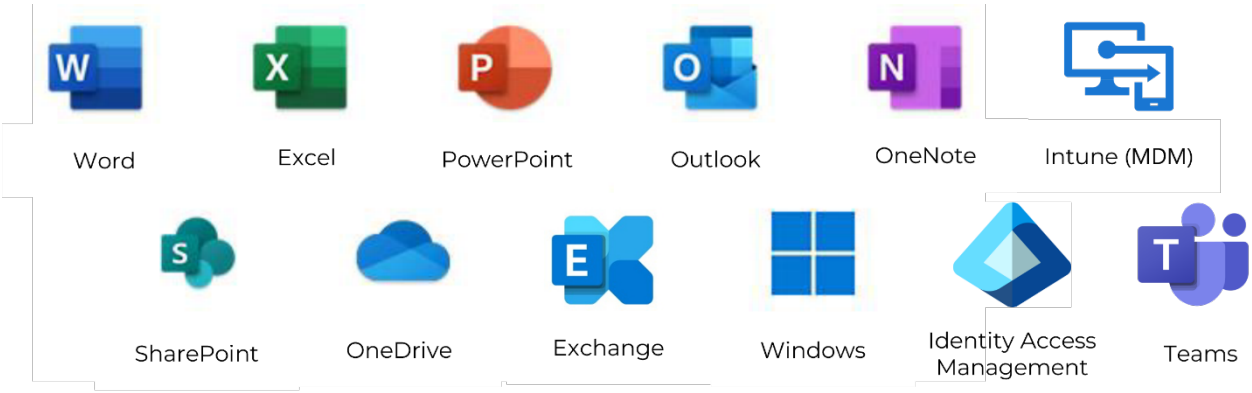


Abbildung 1: Microsoft-Services, die im Rahmen der vorliegenden Studie untersucht wurden.

3 Vorgehen und Methodik

Für die Erarbeitung der Studie wurde eine Projektorganisation gemäss HERMES gewählt, siehe Abbildung 2. Die Planung mit der Übersicht der Meilensteine und Aktivitäten zwischen den einzelnen Meilensteinen ist in Abbildung 3: Meilensteine und Aktivitäten während der Erarbeitung der Studie

dargestellt. Im gesamten Zeitfenster fanden jede zweite Woche Abstimmungsbesprechungen zwischen der Projektleitung und den Studienautoren statt.

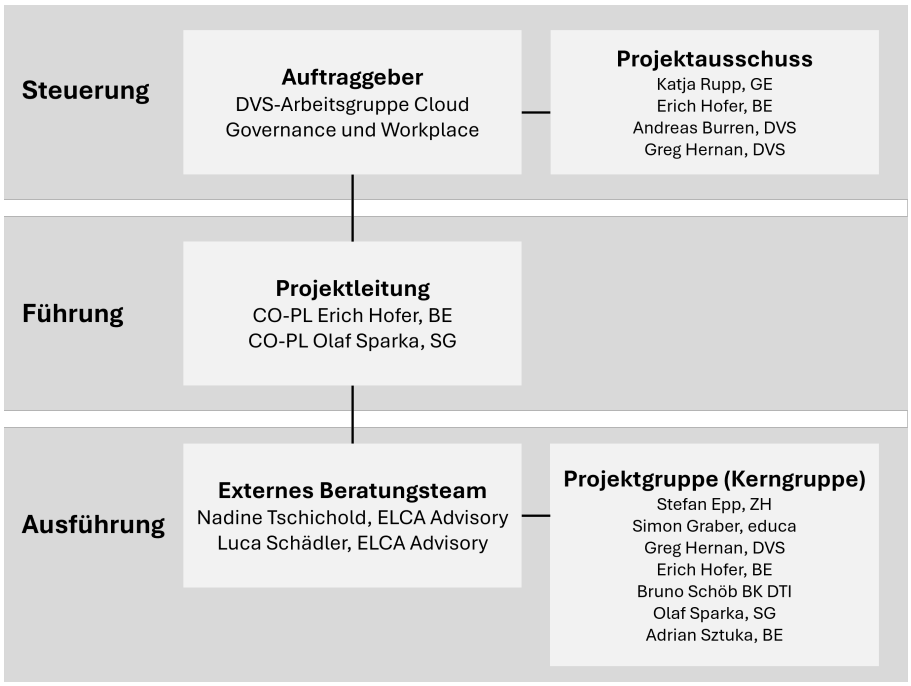


Abbildung 2: Projektorganisation für die Erarbeitung der Studie

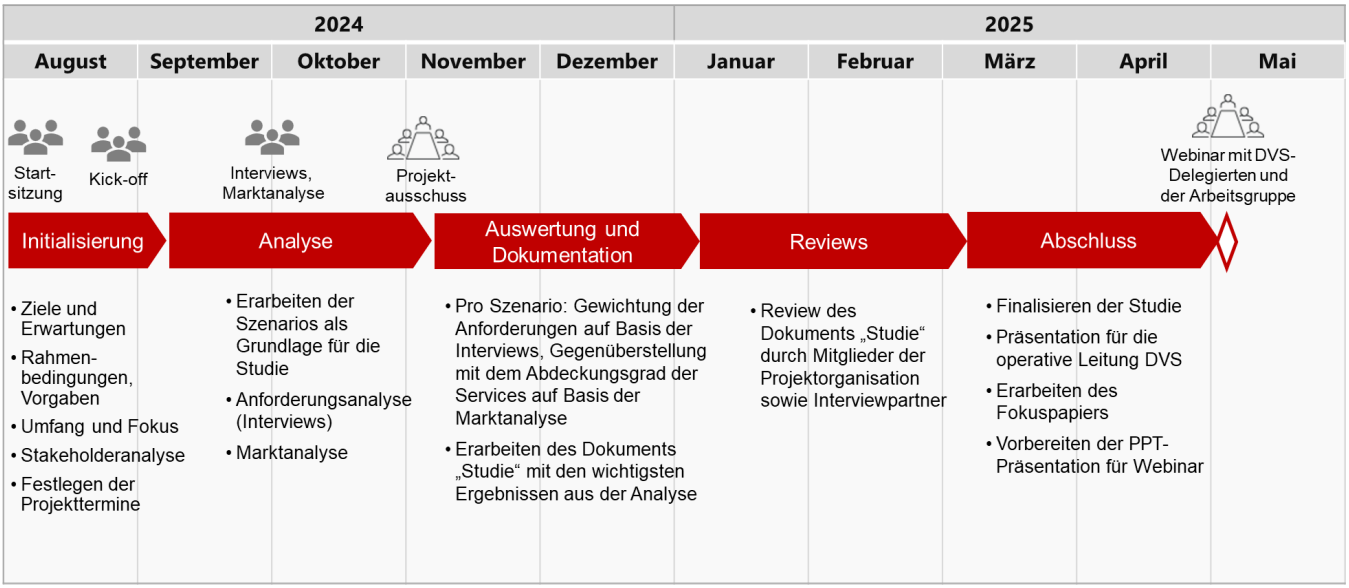


Abbildung 3: Meilensteine und Aktivitäten während der Erarbeitung der Studie

Das Vorgehen basierte auf den folgenden Schritten:

- **Identifikation von Lösungsansätzen** zur Gestaltung der Architektur mit alternativen Services:
  Diese Lösungsansätze bieten verschiedene Optionen zur Integration alternativer Services in die bestehende IT-Infrastruktur der Verwaltung, siehe Kap. 5.
- **Anforderungserhebung** auf Basis der zwei Szenarien (siehe Kap. 2) bei Vertretern von Verwaltungseinheiten, die sich freiwillig gemeldet hatten:
  Im ersten Schritt wurden die Anforderungen der Verwaltungen an alternative Lösungen erfasst. Interviews mit Vertretern der öffentlichen Verwaltung wurden durchgeführt, um die wesentlichen Bedürfnisse und Prioritäten zu identifizieren. Dabei wurde die Wichtigkeit der Anforderungen je nach Szenario (IT-SCM und Exit, siehe Kap. 4) klassifiziert. Die Anforderungen wurden für jedes Szenario separat betrachtet, um die jeweiligen Bedürfnisse genau verstehen zu können.
- **Marktanalyse** mittels der Durchführung einer schriftlichen Umfrage bei potenziellen europäischen Anbietern für komplette Produkt-Suiten sowie Anbietern von alternativen Einzelservices für Front- und Backend-Lösungen:
  Dafür wurden die Anbieter gebeten, die Abdeckung der spezifischen Anforderungen in Bezug auf ihre angebotenen Lösungen zu bewerten und, allgemeine verfügbare Informationen zu ihren Produkten zu bestätigen.
- **Gegenüberstellung der Ergebnisse aus der Anforderungserhebung und der Marktanalyse**:
  Im letzten Schritt wurden die Ergebnisse aus der Anforderungserhebung mit den Ergebnissen der Marktanalyse verglichen.

Abgrenzung

Es ist zu beachten, dass die Studie keine konkreten Empfehlungen für Umsetzungen oder Lösungen enthält und auch keine Überprüfung der technischen Machbarkeit alternativer Lösungen vornimmt. Des Weiteren wird keine Bewertung von alternativen OSS-Produkten oder deren Vergleich vorgenommen. Vielmehr beschränkt sich die Studie darauf, eine Übersicht über die derzeit verfügbaren Lösungen zu bieten und diese den Anforderungen gegenüberzustellen, die im Rahmen von Interviews mit Vertretern von einzelnen Kantonen und Gemeinden erhoben wurden.

4 Untersuchte Szenarien

In diesem Kapitel werden die beiden zu betrachtenden Szenarien: «IT-SCM» und «Exit» beschrieben. Diese verfolgen unterschiedliche Ansätze und setzen verschiedene Prioritäten im Hinblick auf die Anforderungen an mögliche alternative (Open Source) Produkte.

4.1 Szenario: «IT-SCM»

In diesem Szenario liegt der Fokus darauf, auf eine unerwartete Nichtverfügbarkeit der Microsoft-Produkte vorbereitet zu sein (Notfallszenario). Ein solcher Ausfall kann durch unvorhergesehene technische Störungen, politische oder regulatorische Veränderungen oder Sicherheits-bedrohungen verursacht werden. Ziel des «IT Service Continuity Managements» (IT-SCM) ist es, in solchen Notsituationen die Kontinuität und Stabilität kritischer IT-Services sicherzustellen. Dabei werden die wesentlichen Anforderungen identifiziert, die im Rahmen eines IT-SCM-Szenarios von zentraler Bedeutung sind und daher durch alternative Produkte unbedingt erfüllt werden müssen.

Dieses Szenario geht davon aus, dass ein vorübergehender Ersatz von Microsoft-Services unter erheblichem Zeitdruck aufgrund externer Zwänge notwendig wird. In einem solchen Fall müsste das IT-SCM-Konzept greifen, um den Betrieb kritischer IT-Services sicherzustellen. Zudem ist es in der heutigen VUCA*-Welt nicht mehr ausreichend, sich ausschliesslich auf vertragliche Regelungen zu verlassen. Organisationen müssen sich proaktiv auf potenzielle Risiken vorbereiten und entsprechende Massnahmen einleiten, um die Kontinuität der IT-Services auch in unvorhergesehenen Situationen zu gewährleisten.

4.2 Szenario: «Exit»

Im Rahmen des Exit-Szenarios wird ein geplanter Übergang von der Nutzung der Microsoft-Servicefamilie zu alternativen Open Source Lösungen betrachtet. Dieses Szenario zielt darauf ab, eine schrittweise und strukturierte Ablösung von Microsoft-Services zu ermöglichen, um die Abhängigkeit von proprietären Softwarelösungen (speziell Microsoft) zu verringern. Eine Kündigung durch die Institutionen kann auch aufgrund von Änderungen der Services notwendig sein, weil die neuen Bedingungen für die öffentlichen Institutionen nicht mehr tragbar sind, z.B. Integration von Copilot in verschiedenen Microsoft-Services und die damit zusammenhängende Datenschutz-Problematik.

Der Fokus in diesem Szenario liegt auf der Identifizierung geeigneter alternativer Produkte, die die spezifischen Anforderungen der öffentlichen Verwaltung erfüllen. Da der Wechsel zu Alternativlösungen ohne externe Zwänge und Zeitdruck erfolgt, kann dieser geplant und schrittweise umgesetzt werden. Um die Akzeptanz durch die Benutzer sicherzustellen, ist es erforderlich, dass die Alternativen mindestens die gleiche Qualität und einen vergleichbaren oder besseren Funktionsumfang bieten wie die derzeitigen Microsoft-Services, um die Bedürfnisse der Verwaltung umfassend zu erfüllen.

---

* VUCA ist ein Akronym, das für Volatilität (Volatility), Unsicherheit (Uncertainty), Komplexität (Complexity) und Mehrdeutigkeit (Ambiguity) steht. Es beschreibt die dynamischen und oft unvorhersehbaren Herausforderungen, mit denen Unternehmen und Führungskräfte in der heutigen Welt konfrontiert sind.

Hinweis: Stand heute würde eine Kündigung der Services durch Microsoft die meisten Institutionen vor extreme Schwierigkeiten stellen, weil die Kündigungsfrist im schlimmsten Fall nur 6 Monate beträgt. Deshalb ist es wichtig, dass bereits geeignete Massnahmen definiert und Vorbereitungen getroffen werden, damit ein Wechsel erfolgen kann, wenn auch mit Einschränkungen.

5 Untersuchte Lösungsansätze

In dieser Studie wurden drei Lösungsansätze identifiziert, die aufzeigen, wie die Architektur mit alternativen Open Source Services gestaltet werden kann.

5.1 Architekturvarianten

Die folgenden Abbildungen stellen die möglichen Lösungsansätze dar.

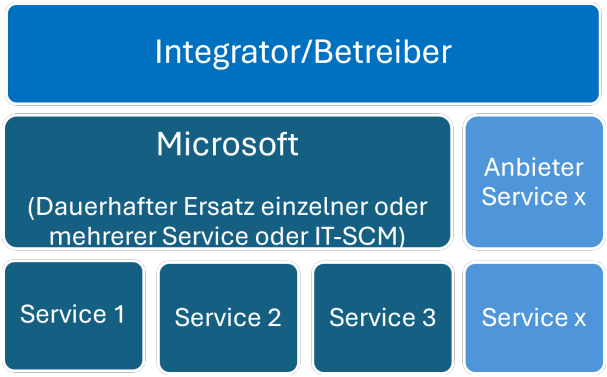


Abbildung 4: Lösungsansatz 1 «Hybride Architektur»

Hybride Architektur:

Einzelne Produkte (hellblau) werden als alternative Serviceoptionen analysiert. Hierbei wird geprüft, inwiefern diese Produkte in die bestehende IT-Infrastruktur integriert werden können, sei es durch ein Drittunternehmen oder durch Eigenleistungen der Verwaltung.

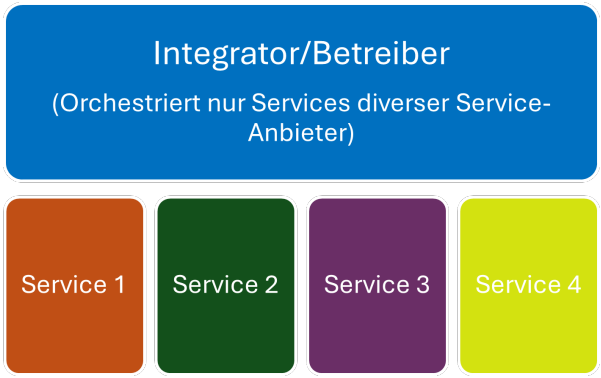


Abbildung 5: Lösungsansatz 2 «Multi-Vendor Architektur»

Multi-Vendor Architektur:

Services verschiedener Anbieter decken den Funktionsumfang der Microsoft-Services ab. In diesem Szenario können unterschiedliche Lösungen kombiniert werden, um die erforderlichen Funktionen bereitzustellen. Die Integration dieser verschiedenen Services kann sowohl durch externe Dienstleister, als auch durch interne Ressourcen erfolgen.

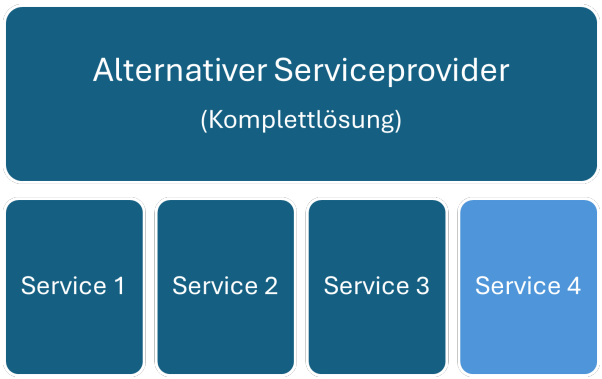


Abbildung 6: Lösungsansatz 3 «Single-Vendor Architektur»

Single-Vendor Architektur:

Ein Anbieter deckt den gesamten Funktionsumfang der Microsoft-Services ab. Dieser Anbieter kann bei Bedarf zusätzliche Services von Drittanbietern integrieren und übernimmt die Verantwortung für die Integration dieser Drittservices.

5.2 Vergleich der Lösungsansätze

Eigenschaft / Kriterium	Hybride Architektur	Multi-Vendor Architektur	Single-Vendor Architektur
Anzahl Lieferanten	Einer oder mehrere	Mehrere	Einer
Verantwortung der Integration der Produkte	Selbst oder Dritt-Unternehmen (nicht Microsoft)	Selbst oder Dritt-Unternehmen	Anbieter
Flexibilität und Anpassungs-fähigkeit	Hoch, durch selektive Wahl von Alternativen zu Microsoft-Lösungen, Mögliche Einschränkungen durch Integrator/Betreiber	Sehr hoch, mit der Möglichkeit, beste Lösungen auszuwählen	Gering, da alle Services von einem Anbieter kommen
Integrations-aufwand	Mittel bis hoch, da die Integration des jeweiligen Services nicht durch Microsoft erfolgt	Sehr hoch, da mehrere Lösungen integriert werden müssen	Niedrig, da der Lieferant die Lösung liefert
Komplexität	Mittel, aufgrund der Notwendigkeit der Integration	Sehr hoch, da die Orchestrierung vieler Lieferanten erforderlich ist und die Lösungen einzeln integriert werden müssen	Niedrig, da alle Services zentralisiert sind
Abhängigkeit vom Anbieter	Gering bis mittel, durch hybride Lösung	Gering, da Anbieter diversifiziert werden	Sehr hoch, da nur ein Anbieter gewählt wird
Langfristige Skalierbarkeit	Hoch, durch schrittweise Anpassung und Integration	Sehr hoch, da neue Anbieter flexible integriert werden können	Mittel, da der Anbieter möglicherweise nicht alle künftigen Anforderungen abdecken kann

Tabelle 1: Lösungsansätze im direkten Vergleich

Jede Architektur bietet spezifische Vorteile, die je nach den strategischen Zielen der Organisation und der Risikobereitschaft gewichtet werden müssen.

5.3 Qualitätskriterien für die Auswahl der Lösungsansätze

Für die Bewertung der Lösungsansätze sind verschiedene Qualitätskriterien entscheidend.

Wichtige Kriterien sind:

1. **Eignung**: Die Lösung bzw. die Service-Architektur muss den spezifischen Anforderungen und Prozessen der Verwaltung entsprechen und flexibel auf gesetzliche oder organisatorische Änderungen reagieren können.
2. **Kosten**: Neben den Anschaffungskosten sind auch die langfristigen Wartungs-, Lizenz- und Supportkosten zu berücksichtigen, um die Wirtschaftlichkeit der Lösung im Sinne der Total Cost of Ownership (TCO) sicherzustellen.
3. **Technische Anforderungen**: Die eingesetzten Produkte müssen stabil, zuverlässig und kompatibel mit bestehenden Systemen sein, offene Standards unterstützen, um Interoperabilität und Effizienz zu gewährleisten.
4. **Langfristige Skalierbarkeit:** Die Lösung muss so gestaltet sein, dass sie zukünftige Anforderungen hinsichtlich steigender Nutzerzahlen, wachsender Datenmengen und neuer technischer Anforderungen flexibel und ohne grundlegende Änderungen bewältigen kann.
5. **Verfügbare Ressourcen und Wissen:** Die Lösung muss auf vorhandenen personellen und technischen Ressourcen basieren oder durch Schulungen und externe Unterstützung ergänzt werden, um einen reibungslosen Betrieb und Weiterentwicklung sicherzustellen.
6. **Usability**: Eine benutzerfreundliche Oberfläche erleichtert den Zugang, reduziert Schulungsaufwand und Fehler, was die Effizienz steigert.
7. **Benutzerakzeptanz**: Hohe Akzeptanz unter den Mitarbeitenden fördert eine produktive Nutzung und reibungslose Integration neuer Lösungen.
8. **Sicherheit**: Um den Schutz sensibler Daten zu gewährleisten, sind Zugriffskontrollen und Schutzmechanismen gegen Cyber-Bedrohungen notwendig.
9. **Datenschutz**: Die Architektur muss Datenschutz-konform sein und sichere, transparente Mechanismen zum Schutz personenbezogener Daten bieten.
10. **Souveränität**: Die Unabhängigkeit von einzelnen Anbietern ist essenziell, um digitale Souveränität und Kontrolle über Daten und Systeme zu wahren.

6 Anforderungserhebung

Um die Relevanz verschiedener Anforderungen im Kontext potenzieller Alternativlösungen zu ermitteln, wurden Interviews mit öffentlichen Verwaltungen durchgeführt. Das Ziel dieser Gespräche war es, die Vollständigkeit der Anforderungen sicherzustellen. Zudem wurde deren Wichtigkeit in den beiden Szenarien *IT-SCM* und *Exit* separat erfasst, um gezielt auf unterschiedliche Bedarfe einzugehen und die Relevanz der Anforderungen in Abhängigkeit von den Szenarien zu berücksichtigen.

6.1 Vorgehen

Das Vorgehen für die Anforderungsanalyse war wie folgt:

1. **Erfassung der Anforderungen an Microsoft-Services:** Auf Basis von Literatur-Recherchen wurden die technischen Anforderungen an die Microsoft-Services erfasst. Diese Anforderungen wurden anschliessend verallgemeinert und zusammengefasst, sodass sie weniger technisch ausgerichtet sind und aus Managementsicht bewertet werden können.
2. **Definition der Anforderungen an Anbieterfirmen:** Um die relevanten Eigenschaften potenzieller Lösungsanbieter in der Studie zu berücksichtigen, wurde eine Liste von Anforderungen definiert (siehe Kap. 7.5).
3. **Rekrutierung von Teilnehmern an der Anforderungsanalyse:** Der Aufruf zur Teilnahme an der Anforderungsanalyse erfolgte im Rahmen der «Online Cloud und Workplace Tagung» vom 29.08.2024 von DVS. An der Tagung wurden die Ziele, das Vorgehen und der Umfang der Studie vorgestellt. Am 23.09.2024 erfolgte ein zweiter Aufruf per E-Mail. Alle Interessenten, die sich gemeldet hatten, wurden bei den Interviews berücksichtigt, siehe Tabelle 2.
4. **Vorbereitung und Durchführung der Anforderungsanalyse:** Die Anforderungsanalyse erfolgte im Rahmen von Online-Interviews. Die Listen der Anforderungen (siehe Punkt 1 und 2) wurden vorab an die Interviewpartner geschickt. Die Anforderungslisten wurden vor den Interviews ausgefüllt retourniert. Im Rahmen der Interviews wurden die Anforderungen besprochen, die Wichtigkeit aus Sicht der Interviewpartner erhoben und bei Bedarf kommentiert. Einzelne Anforderungen wurden mit den Interviewpartnern vertieft besprochen, insbesondere diejenigen Anforderungen, deren Wichtigkeit stark unterschiedlich bewertet wurden.
5. **Konsolidierung der Ergebnisse:** Die Ergebnisse aus den Interviews wurden in der Datei im Anhang A [1] konsolidiert. Pro Interviewpartner wurde die Einschätzung der Wichtigkeit explizit festgehalten. Die Kommentare aus den Interviews wurden zusammengefasst.

Anspruchsgruppe	Berücksichtigung im Projekt	Vertretung	Interview
Digitale Verwaltung Schweiz	Auftraggeber	Arbeitsgruppe Cloud Governance und Workplace	Kein Interview, nur Gestaltung der Anforderungsanalyse inkl. Review der Anforderungsliste
Kantone	• Kanton Basel-Stadt • Kanton Graubünden • Kanton Tessin • Kanton Genf • Kanton Appenzell Ausserrhoden	• Urs Bühler (BL) • Reto Rauch & Mirko Demarmels (GR) • Rudi Belotti (TI) • Katja Rupp (GE) • Christoph Schwalm (AR)	• 17.10.24 • 16.10.24 • 21.10.24 • 16.10.24 • 16.10.24
Gemeinden	• Stadt Zürich	• Werner Kipfer (Stadt ZH)	• 17.10.24

Tabelle 2: Anspruchsgruppen und Interviewpartner

6.2 Inhalt

Die Anforderungsanalyse gliedert sich in verschiedene Themengebiete, die jeweils zentrale Anforderungen an die betrachteten Microsoft-Services abdecken. Die untersuchten Themengebiete sind:

- **Betriebssystem**
- **IAM** (Benutzerverwaltung und LDAP)
- **Office**
- **E-Mail**
- **Datenablage und Kollaboration** (z. B. Teams, SharePoint)
- **Kommunikation** (z. B. Chat, Audio- und Videokonferenzen)
- **Mobile Device Management** (MDM)
- **Lösungsunabhängige Anforderungen** (Usability, UI, UX, etc.)
- **Telefonie**
- **RAS / VDI Büroautomatisierung**

6.3 Erkenntnisse aus den Interviews

Die Ergebnisse aus den Interviews gemäss Tabelle 2 wurden in einer Excel-Tabelle zusammengetragen (siehe Anhang A [1]).

Im ersten Teil der Interviews wurden Informationen zu allgemeinen Themen eingeholt. Die Tabelle 3 beinhaltet die Zusammenfassung der Antworten auf diese Interviewfragen.

Im zweiten Teil der Interviews haben die Interview-Teilnehmenden die Anforderungen an die einzelnen Microsoft-Services bezüglich deren Wichtigkeit eingestuft. Dabei wurde festgestellt, dass das IT-SCM-Szenario von den Teilnehmern hinsichtlich des betrachteten Zeitraums unterschiedlich wahrgenommen wird. Während einige Interviewpartner einen Zeitraum von zwei Wochen angaben, in dem die IT-SCM-Lösung greifen muss, bezogen sich andere auf eine Zeitspanne von bis zu 48 Monaten. Die längere Zeitspanne wurde damit begründet, dass eine definitive Lösung evaluiert, integriert, implementiert und alle Mitarbeitenden geschult werden müssen, ein kürzeres Zeitfenster deshalb nicht realistisch sei.

Es zeigte sich deutlich, dass die Anforderungen an den Funktionsumfang der Services im IT-SCM-Szenario tendenziell als weniger wichtig eingestuft wurden. Dies liegt daran, dass in einem solchen Szenario die IT-Services weiterhin verfügbar bleiben müssen und daher Abstriche bei bestimmten Anforderungen akzeptiert werden. Zudem wurde argumentiert, dass es sich hierbei um eine Übergangsphase handelt, die nicht als endgültige Lösung zu betrachten ist. Entsprechend können einige Anforderungen vorübergehend entfallen.

Im Gegensatz dazu wurde im Exit-Szenario die Mehrzahl der Anforderungen als sehr wichtig eingestuft. Dies ist nachvollziehbar, da eine alternative Lösung nicht akzeptiert wird, wenn sie die bestehenden Anforderungen nicht erfüllt oder nur einen geringeren Abdeckungsgrad bietet.

Stand der Arbeiten in den eigenen Organisationseinheiten	
Pläne zur Evaluierung oder Ablösung von Microsoft 365	Etwa die Hälfte der Befragten prüft derzeit Alternativen zu Microsoft 365 oder plant solche Evaluierungen. Die andere Hälfte sieht keine Notwendigkeit, Microsoft 365 durch andere Lösungen zu ergänzen oder zu ersetzen.
Wichtigkeit von Alternativen zur Reduktion der Abhängigkeit	Eine Mehrheit stuft die Entwicklung von Alternativen als «wichtig» oder «teilweise wichtig» ein, um die Abhängigkeit von Microsoft zu reduzieren. Lediglich eine Minderheit sieht hier keinen Handlungsbedarf. Ebenfalls erwähnten einige Teilnehmer, dass Regierungsräte bei der Einführung von M365 im Kanton die Erarbeitung einer Exit-Strategie verlangen.
IT Service Continuity Management (IT-SCM)	
Relevanz einer IT-SCM-Strategie zu M365	Eine grosse Mehrheit erkennt die Bedeutung einer IT-SCM-Strategie für Microsoft 365 an, auch wenn der Reifegrad der Strategien variiert. Einige Kantone haben solche Strategien bereits umgesetzt, während andere nur Teilaspekte behandeln.
Einsatz von Alternativen zu Microsoft 365	Einige Kantone setzen Alternativen ein, z. B. Open Source Software, um Abhängigkeiten zu reduzieren. Die Zufriedenheit mit diesen Alternativen wird unterschiedlich bewertet. Häufig wird festgestellt, dass diese Lösungen im Funktionsumfang oder in der Stabilität nicht an Microsoft 365 heranreichen.

Exit-Strategien für Microsoft 365	
Ausstieg aus Microsoft 365	Nur sehr wenige Befragte haben konkrete Exit-Strategien entwickelt oder in Erwägung gezogen. In den meisten Fällen fehlen definierte Optionen oder Partner, die bei einem potenziellen Ausstieg unterstützen könnten. Der Fokus liegt stärker auf der Ergänzung von M365 durch alternative Lösungen als auf einem vollständigen Wechsel.
Politische und regulatorische Massnahmen	
Initiativen zur digitalen Souveränität	In einigen Kantonen und Gemeinden wurden politische Initiativen gestartet, um die Abhängigkeit von Microsoft-Services zu hinterfragen und digitale Souveränität zu stärken. Diese Initiativen zielen häufig darauf ab, Open Source Software stärker zu fördern oder regulatorische Vorgaben zur Nutzung von Cloud-Services zu etablieren.
Massnahmen zur Förderung digitaler Souveränität	Einige Kantone und Gemeinden setzen gezielt auf den Einsatz von Open Source Software (OSS), allerdings spielt OSS insgesamt nur eine untergeordnete Rolle. Massnahmen zur Förderung der digitalen Souveränität stehen oft erst am Anfang.
Regulatorische Massnahmen zu M365	Regulatorische oder politische Massnahmen im Zusammenhang mit der Nutzung von Microsoft 365 wurden in einigen Fällen ergriffen. Diese werden jedoch unterschiedlich behandelt und umgesetzt.

Tabelle 3: Zusammenfassung der Antworten auf die allgemeinen Interviewfragen

7 Marktanalyse

Mit der durchgeführten Marktanalyse (siehe Anhang A [1]) wurde eine Übersicht über verschiedene Open Source Alternativlösungen zu den Microsoft-Produkten erstellt.

7.1 Vorgehen

In einem ersten Schritt wurden mit einer umfassenden Internet-Recherche potenzielle Open Source Alternativlösungen zu Microsoft-Services identifiziert und eine Liste der verschiedenen Anbieter und deren Services erstellt. Parallel dazu wurde die Liste der Anforderungen an die Microsoft-Services erarbeitet, die mit Vertretern einzelner Kantonen und Gemeinden im Rahmen von Interviews bereinigt wurde.

In einem zweiten Schritt wurde die Anforderungsliste im Rahmen eines "Request for Information" (RFI) an ausgewählte Anbieter geschickt mit der Bitte, diese innerhalb von 3 Wochen (30.10 bis 18.11.2024) zu beantworten. Die Kriterien und Eingrenzungen für die Auswahl der Firmen werden in Kap. 7.3 detailliert erläutert.

Im Rahmen der strukturierten Marktanalyse (s. Anhang A [1]) gaben die Firmen pro Anforderung an, inwieweit ihre Services die jeweiligen Anforderungen erfüllen. Diese Angaben wurden der Wichtigkeit der Anforderungen, die im Rahmen von Interviews aufgenommen wurden, gegenübergestellt.

7.2 Aufbau der Marktanalyse

Als Grundlage für die Marktanalyse wurde ein Fragenkatalog mit dem folgenden Aufbau erstellt:

- **Produktkategorien:**
  - Gesamtlösungen (Suiten)
  - Einzellösungen für das Backend
  - Einzellösungen für das Frontend
- **Funktionsumfang:**
  - Benutzerverwaltung
  - Integrierte Office- und E-Mail-Services
  - Kommunikations- und Videokonferenzlösungen
  - Funktionen für die Zusammenarbeit (z. B. Dokumentenmanagement, Content-Management, Wissensmanagement)
  - Messaging-Funktionen
  - Mobile Device Management (MDM) zur Erfüllung moderner Arbeitsanforderungen
- **Anbieterinformationen:**
  - Produktname
  - Name des Anbieters
  - Internetadresse
  - Herkunftsland des Anbieters
  - Open Source Verfügbarkeit des Produkts
  - Bereitstellungsmodelle (z. B. SaaS oder On-Premises)
  - Unterstützte Betriebssysteme

7.3 Auswahl der Anbieter für die Marktanalyse

Folgende Kriterien wurden für die Wahl der Firmen, die im Rahmen des RFI angefragt wurden, herangezogen:

- Angebot von Gesamtlösungen*
- Auf Basis von Open Source Software
- Firmensitz in der Schweiz oder in der EU

In dieser Studie liegt der Fokus auf der Betrachtung von Gesamtlösungen (Lösungsansatz 3 in Kap. 5.1), d.h. Anbieter von umfassenden und integrierten Lösungen. Die übrigen Lösungsvarianten, die auf Einzellösungen basieren, wurden bereits in den Studien der Berner Fachhochschule (BFH) behandelt (siehe Beilagen [B1] und [B2]). Eine detaillierte Beschreibung der Strategie für die Wahl eines solchen Ansatzes und auch das Vorgehen der Multivendor-Lösungsvariante wurde von Schleswig-Holstein erarbeitet (siehe Beilage [B3]).

Ein Firmensitz in der Schweiz oder in der EU ist vor allem wichtig, um die Einhaltung spezifischer rechtlicher Rahmenbedingungen und Datenschutzanforderungen sicherzustellen.

Tabelle 4 gibt die angefragten Firmen und ihre Produkte wieder. Nicht alle Firmen haben auf das RFI geantwortet (siehe Tabelle 4) und die Qualität der Ausführungen variierte.

Firma	Produkt	Antwort erhalten am
Virtual Network Consult (VNC) AG	VNCLagoon	14.11.2024
ZenDiS GmbH	openDesk	04.02.2025
Infomaniak Genf AG	kSuite	19.12.2024
EGroupware GmbH	EGroupWare	11.11.2024
Hostpoint AG	E-Mail und Office Lösung	Keine Antwort erhalten

Tabelle 4: Liste der angefragten Firmen und ihre Produkte

ZenDiS GmbH hat die RFI-Anfrage mit grosser Verspätung beantwortet. Insbesondere in Deutschland werden sie mit Anfragen überhäuft, was zu langen Reaktionszeiten auf neue Anfragen führt.

Auch die Unternehmen Hostpoint und Unblu wurden im Rahmen des RFI kontaktiert. Eine Antwort von Hostpoint blieb aus. Unblu hat ausdrücklich kein Interesse an der Beantwortung bekundet.

7.4 Eigenschaften der Services

Die angebotenen Services müssen die besonderen Anforderungen und Regularien des öffentlichen Sektors erfüllen und gleichzeitig wirtschaftlich tragbar sein, sowohl kurzfristig als auch langfristig. Zu den wesentlichen Eigenschaften, die näher zu betrachten sind, gehören:

- **Funktionsumfang:** Die Funktionen der Software-Lösungen müssen die aktuellen und zukünftigen Anforderungen der öffentlichen Verwaltung abdecken. Die Kernfunktionalität der Microsoft-Produkte müssen abgedeckt werden.
- **Bereitstellungsmodell (SaaS, On-Prem):** SaaS bietet Skalierbarkeit und schnelle Implementierung, während On-Prem mehr Kontrolle, aber oft höhere Kosten bietet.
- **Datenschutz- und Informationssicherheit (private/dedizierte Cloud):** Diese Service-Modelle bieten hohe Sicherheit und erfüllen Compliance-Anforderungen, wie z.B. der Datenschutz- und Informationssicherheit-Gesetze.
- **Open Source:** Bietet Transparenz und Unabhängigkeit, fördert Anpassungen durch die Open Source Community und Datensouveränität.
- **Lizenzmodell:** Ein klares Lizenzmodell ist wichtig für transparente Kostenkalkulation und langfristige Budgetplanung**.**
- **Dienstleistungen:** Die Abdeckung der relevanten Dienstleistungen wie z.B. Integration und Konfiguration der Software-Produkte sowie Support-Leistungen und allgemeine Benutzerunterstützung sind entscheidende Eigenschaften, die erfüllt werden müssen.
- **Betriebskosten:** Langfristige Finanzierbarkeit des Betriebs muss gewährleistet sein.
- **Vertragsmodell:** Flexibilität im Vertrag ist wichtig, um Abhängigkeiten und unvorhergesehene Kosten zu vermeiden.

7.5 Eigenschaften der Firmen

Um eine fundierte Entscheidung für den Einsatz von IT-Lösungen treffen zu können, ist nicht nur eine Analyse der Produkteigenschaften, sondern auch eine Bewertung der jeweiligen Anbieterfirmen von grosser Bedeutung. Die Merkmale der Unternehmen hinter den Lösungen geben Aufschluss darüber, ob eine langfristige und verlässliche Zusammenarbeit gewährleistet werden kann und ob das Unternehmen auch zukünftige Anforderungen erfüllen und mit den technologischen Entwicklungen mithalten kann.

Zu den relevanten Eigenschaften der Anbieterfirmen zählen:

- **Firmensitz und zukünftige Pläne:** Der Unternehmensstandort beeinflusst Datenschutz und Compliance. Geplante Veränderungen, wie ein Umzug, können rechtliche Rahmenbedingungen und Serviceverfügbarkeit betreffen.
- **Grösse des Unternehmens:** Die Grösse des Unternehmens gibt einen Hinweis auf die verfügbaren Ressourcen für die Weiterentwicklung und Support der Produkte und Services.
- **Marktsicherheit:** Die wirtschaftliche Stabilität des Unternehmens ist wichtig, um Risiken durch mögliche Insolvenz und deren Auswirkungen auf die Servicekontinuität zu vermeiden.
- **Abhängigkeit vom Anbieter:** Eine zu starke Abhängigkeit kann zu einem zentralen Risikofaktor werden. Die Gestaltungs- und Einflussmöglichkeiten beim Bezug der Services und Betrieb der Lösungen ist ein relevanter Faktor, der bei Verhandlungen mit Anbietern zu berücksichtigen ist.
- **Kundenkreis:** Ein stabiler, grosser Kundenstamm, idealerweise auch mit Kunden im öffentlichen Sektor, zeigt, dass die Lösung praxiserprobt und geeignet für die Anforderungen der Verwaltung ist.

Ein weiterer wesentlicher Faktor ist die Grösse und das Aktivitätsniveau der Open Source Community. Je grösser die Community mit gemeinsam definierten Standards ist und je mehr Unternehmen aktiv daran teilnehmen, desto höher ist die Unabhängigkeit von einzelnen

Anbietern. Dadurch können öffentliche Institutionen wie Kantone und Gemeinden Dienstleistungen von verschiedenen Firmen beziehen, was den Wechsel zwischen Anbietern erleichtert.

7.6 Ergebnisse der Marktanalyse

In der folgenden Tabelle 5 sind die Ergebnisse der Marktanalyse auf Basis der Rückmeldungen der angefragten Firmen zusammengefasst. Der Abdeckungsgrad der Anforderungen basiert auf den Angaben der jeweiligen Anbieter der Lösungen und wurde nicht explizit geprüft.

Der Tabelle kann ebenfalls entnommen werden, wie viele Anforderungen pro Anforderungsgruppe vollständig abgedeckt sind.

Anforderungsgruppe	Erfüllungsgrad der Anforderungen			
	EGroupware	VNCLagoon	kSuite	openDesk
Lösungs-unabhängige Anforderungen	**Mehrheitlich** (5 von 9 vollständig)	**Fast vollständig** (8 von 9 vollständig)	**Fast vollständig** (8 von 9 vollständig)	**Fast vollständig** (7 von 9 vollständig)
Office	**Mehrheitlich** (3 von 5 vollständig)	**Fast vollständig** (4 von 5 vollständig)	**Fast vollständig** (4 von 5 vollständig)	**Vollständig**
E-Mail	**Mehrheitlich** (2 von 4 vollständig)	**Vollständig**	**Fast vollständig** (3 von 4 vollständig)	**Fast vollständig** (3 von 4 vollständig)
Kollaboration	**Mehrheitlich** (2 von 4 vollständig)	**Vollständig**	**Vollständig**	**Vollständig**
Betriebssystem	**Teilweise** (1 von 4 vollständig, 3 teilweise)	**Fast vollständig** (3 von 4 vollständig)	**Teilweise** (1 von 4 vollständig, 3 teilweise)	**Mehrheitlich** (2 von 4 vollständig)
Clients	**Teilweise** (0 von 2 vollständig, 1 teilweise)	**Mehrheitlich** (1 von 2 vollständig)	**Teilweise** (0 von 2 vollständig, beide teilweise)	**Mehrheitlich** (1 von 2 vollständig)
IAM	**Teilweise** (1 von 6 vollständig, 4 teilweise)	**Vollständig**	**Vollständig**	**Fast vollständig** (5 von 6 vollständig)
RAS / VDI **Remote Access und Virtualisierung**	**Teilweise** (0 von 2 vollständig, beide teilweise)	**Vollständig**	**Teilweise** (0 von 2 vollständig, 1 teilweise)	**Teilweise** (0 von 2 vollständig, 1 teilweise)

Anforderungsgruppe	Erfüllungsgrad der Anforderungen			
	EGroupware	**VNCLagoon**	**kSuite**	**openDesk**
Mobile Device Management	**Nicht abgedeckt**	**Vollständig**	**Vollständig**	**nicht Teil von openDesk**
Telefonie	**Teilweise** (2 von 7 vollständig, 3 teilweise)	**Mehrheitlich** (3 von 7 vollständig)	**Teilweise** (2 von 7 vollständig)	**nicht Teil von openDesk**

Tabelle 5: Abdeckungsgrad der Anforderungsgruppen

Die detaillierten Ergebnisse der Marktanalyse befinden sich im Anhang A [1], wo die Anforderungen und ihre Wichtigkeit dem Abdeckungsgrad der verschiedenen Lösungen gegenübergestellt ist.

Fazit: Keines der befragten Unternehmen bietet eine Lösung an, die alle Anforderungsgruppen vollständig abdeckt. Daher ist die Implementierung einer umfassenden Gesamtlösung ohne Kompromisse derzeit nicht möglich.

Erkenntnisse Kundenseite:

Auf der Kundenseite besteht die Herausforderung darin, dass standardisierte Lösungen bevorzugt werden, um den Aufwand für individuelle Anpassungen und Customizing zu minimieren. Ziel ist es, einheitliche Lösungen zu schaffen, die nicht zu einer Vielzahl unterschiedlicher Versionen führen und dadurch die Komplexität in der Umsetzung und im Betrieb reduzieren. Dies erfordert jedoch eine stärkere Abstimmung und die Schaffung interkantonaler Standards (z. B. eCH-Standards), um den Bedarf an individuellen Anpassungen für jeden einzelnen Kanton zu verringern.

Erkenntnisse Anbieterseite:

Auf der Anbieterseite ist zu prüfen, ob sie in der Lage sind, die Anforderungen mehrerer Kantone gleichzeitig zu bearbeiten und die notwendigen Ressourcen für Support und Implementierungsprojekte bereitzustellen. Die fehlenden interkantonalen Standards stellen eine besondere Herausforderung dar, da jeder Kanton individuelle Anpassungen verlangt, was den Aufwand für Anbieter erheblich erhöht. Es muss sichergestellt werden, dass die Anbieter nicht nur die technische Umsetzung bewältigen können, sondern auch langfristig verlässlichen Support und Betreuung garantieren.

8 Open Source Alternativen zu Microsoft Services: Übersicht

Fragestellung: Welche OSS-Alternativen zu Microsoft Services stehen heute zur Verfügung?

Variante «Single-Vendor Architektur»

Die Marktanalyse (s. Kap. 7) hat gezeigt, dass prinzipiell verschiedene OSS-Alternativen zu den Microsoft-Services auf dem Markt verfügbar sind. Jedoch deckt aktuell keine dieser Alternativen den gesamten Funktionsumfang aller relevanten Microsoft-Services ab. Es existieren jedoch Anbieter, die ihre Produkte gezielt weiterentwickeln, um Microsoft-Services funktional näherzukommen. Ein Beispiel hierfür ist das Zentrum Digitale Souveränität (ZenDiS), das sich zu 100% im Besitz öffentlicher Institutionen in Deutschland befindet. Um die Eignung und Leistungsfähigkeit der ZenDiS-Services mit dem Produkt openDesk zu prüfen, hat die Bundeskanzlei mit «PoC Büroautomation mit OSS» (BOSS) ein Pilotprojekt gestartet.

Zusätzlich gibt es in Deutschland Einzelinitiativen auf Ebene einzelner Bundesländer, wie z.B. Schleswig-Holstein. Gemäss der erarbeiteten Strategie (s. Beilage [B3]) werden die Microsoft-Services durch Open Source Alternativen abgelöst. Ein Projekt für die Umsetzung dieser Strategie wurde bereits gestartet.

Solche Initiativen verdeutlichen, dass trotz der bestehenden Lücken verstärkte Bemühungen unternommen werden, um die digitale Souveränität zu fördern und Alternativen zu etablieren.

Variante «Multi-Vendor Architektur» und «Hybride Architektur»

Die Studien der Berner Fachhochschule (s. Beilagen [B1] und [B2]) geben eine Übersicht der Alternativen zu einzelnen Microsoft-Services für Verzeichnisdienste, Datenablage, E-Mail, Kollaboration, Webmail, Office Online, PIM-Datensynchronisation und Kommunikation (Unified Communication). Auch diese Studie zeigt, dass die Anforderungen nicht für alle Services vollumfänglich abgedeckt werden können. Prinzipiell wäre es jedoch möglich, durch die Zusammensetzung von einzelnen Services die Gesamtlösung zu optimieren. Der Integrationsaufwand dazu wäre jedoch hoch, und der Betrieb mit grösseren Risiken verbunden, siehe Kap. 5.2.

Fazit: Ein vollständiger Ersatz der Microsoft-Services durch eine einzige Open Source Gesamtlösung ist derzeit kommerziell nicht verfügbar. Auch die spezifischen Lösungen für einzelne Microsoft-Services bieten nicht die vollständige Funktionalität und deren Einsatz erfordert einen erheblichen Mehraufwand. Jedoch befindet sich der Markt in einem dynamischen Wandel, die aufgrund von aktuellen politischen und technischen Entwicklungen noch beschleunigt werden. Initiativen wie ZenDiS und weitere Unternehmen verfolgen vielversprechende Ansätze, um langfristig souveräne und leistungsfähige Alternativen zu den Microsoft-Services zu entwickeln und den Bedarf daran nachhaltig zu decken.

Auf der Kundenseite stellt sich die Herausforderung, standardisierte Lösungen zu bevorzugen, um den Aufwand für individuelle Anpassungen zu minimieren. Das Ziel ist es, einheitliche Lösungen zu schaffen, die nicht zu einer Vielzahl unterschiedlicher Versionen führen und somit die Komplexität in der Umsetzung und im Betrieb verringern. Dies setzt auch die Schaffung interkantonaler Standards (z. B. eCH-Standards) voraus, um den Bedarf an individuellen

Anpassungen für jeden einzelnen Kanton zu reduzieren und eine breitere Akzeptanz zu erzielen.

Auf der Anbieterseite ist zu prüfen, ob diese in der Lage sind, die Anforderungen mehrerer Kantone gleichzeitig zu bearbeiten und die nötigen Ressourcen für Support und Implementierungsprojekte bereitzustellen. Die fehlende Standardisierung zwischen den Kantonen stellt eine erhebliche Herausforderung dar, da jeder Kanton individuelle Anpassungen verlangt. Dies führt zu einem erheblichen Mehraufwand für Anbieter. Es ist daher wichtig, dass Anbieter nicht nur die technische Umsetzung bewältigen können, sondern auch langfristig verlässlichen Support und kontinuierliche Betreuung bieten, um eine nachhaltige Implementierung und den Betrieb der Lösungen sicherzustellen.

Relevant ist auch das Vorhandensein und die Nutzung einer entsprechenden Open Source Community. Dies erfolgt idealerweise gemeinsam durch die Anbieter und die öffentliche Verwaltung bzw. Vertreter der öffentlichen Institutionen.

9 IT-Service-Continuity mit Open Source Alternativen

Fragestellung: Welche Möglichkeiten bestehen, Microsoft-Services durch Open Source Alternativen zu ergänzen, insbesondere im Kontext eines IT-Service-Continuity-Managements (IT-SCM)?

Die genannten Beispiele von alternativen Services sind nicht abschliessend und basieren auf den Ergebnissen der BFH-Studie (s. Beilagen [B1] und [B2]). Die Betrachtungen beziehen sich primär auf den Ausfall einzelner Services, jedoch ist auch ein gleichzeitiger Ausfall mehrerer Services möglich und muss in die Planung einbezogen werden.

In jedem IT-SCM-Fall ist es die Aufgabe des Notfallteams zu prüfen, welche Services betroffen sind, um geeignete Massnahmen zur Wiederherstellung des Betriebs einzuleiten.

Im Rahmen eines Konzepts zum IT Service Continuity Management (IT-SCM) können teilweise Microsoft-Services durch Open Source Software (OSS)-Alternativen unterstützt werden, um die Verfügbarkeit und Ausfallsicherheit der IT-Services sicherzustellen. Dabei stehen grundsätzlich zwei Ansätze zur Verfügung:

- **Parallelbetrieb:** Die Microsoft-Services und die OSS-Alternativen werden parallel betrieben, die Daten werden laufend synchronisiert. Beide Lösungen werden so aufgesetzt, dass beim Ausfall eines der Services der andere nahtlos bzw. innert Stunden eingesetzt werden kann. Dieser Ansatz gewährleistet eine kontinuierliche Verfügbarkeit der Services und reduziert die Abhängigkeit von einem einzelnen Anbieter.
- **Standby-Bereitstellung:** Die OSS-Services werden so bereitgestellt, dass sie im Notfall mit einigem Aufwand hochgefahren werden können. Unter anderem muss im Notfall ohne verfügbare Daten gearbeitet werden oder die Daten müssen von einem Backup-System zuerst bereitgestellt werden.

Tabelle 6 gibt eine Übersicht der IT-SCM Massnahmen. Unter «kurzfristigen Massnahmen» sind solche gemeint, die bei einem Ausfall eines Service innerhalb von wenigen Tagen eingesetzt werden können. «Dauerhafte Massnahmen» sind solche, die bereits vor dem Service-Ausfall umgesetzt und integriert sein müssen, damit sie bei einem Ausfall-Szenario aktiviert werden können.

Service	Kurzfristige IT-SCM Massnahme	Dauerhafte IT-SCM Massnahme
Identity Access Management (IAM)	keine	Einsatz Meta-Directory für User Identity Management oder Einsatz von mehreren Alternativ-Produkten für Active Directory Funktionalitäten
Clients (Ausfall Betriebssystem)	keine	Bereitstellen einer begrenzten Anzahl von Clients mit alternativen Betriebssystemen

Service	Kurzfristige IT-SCM Massnahme	Dauerhafte IT-SCM Massnahme
Mail	Versand/ Empfang neuer Mails in einem alternativen System	Schattenbetrieb eines anderen Mail-Services mit Synchronisation der Mails
Mobile Device Management (MDM)	keine	Vorbereitung der Einführung eines unabhängigen MDM-Drittproduktes
System Management	keine	Parallelbetrieb eines Alternativ-Systems nicht möglich Vorbereitung der Einführung eines unabhängigen System-Management-Drittproduktes
Remote Access Services/Virtual Desktop Infrastructure (RAS/VDI)	keine	Verzicht auf Remote-Arbeiten bei IT-SCM-Fällen oder Vorbereitung der Einführung eines unabhängigen RAS/VDI-Drittproduktes
Office-Anwendungen	Einsatz von alternativen Services Voraussetzung: Zugriff auf Daten ist noch möglich (lokale Haltung der Daten)	Synchronisierung der Dateien aus Cloud auf Clients
Kollaboration und Datenablage	Arbeiten mit den lokalen Dateien Voraussetzung: Daten sind in standardisierten Formaten vorhanden.	Einstellung, dass Dateien auf dem Client als lokale Kopie gespeichert werden
Kommunikation (Chat, Audio/Video) ohne Telefonie)	Einsatz alternativer Services	Alternativer Service dauerhaft im Betrieb (zusätzlicher Kommunikationskanal)
Telefonie	Einsatz von alternativen Services (z.B. auch via Mobile Telefonie) Voraussetzung: Kontaktdaten sind noch vorhanden	Umleitung der Telefonate auf mobile Telefone; Sicherstellen Verfügbarkeit der mobilen Telefone

Tabelle 6: Übersicht von IT-SCM-Massnahmen

In den folgenden Abschnitten sind mögliche IT-SCM Massnahmen für die einzelnen Services beschrieben.

Fazit: Für einzelne Services können Parallelinstallationen den Ausfall der Microsoft-Services kompensieren (z. B. Mail). Diese sind jedoch in der Regel sehr ressourcenintensiv. Es gibt auch Services, bei denen Parallelinstallationen nicht möglich sind und eine rasche Bereitstellung alternativer Lösungen ebenfalls nicht realistisch ist (z. B. MDM).

Eine fundierte Analyse auf Basis des Risikomanagements ist entscheidend für die Bewertung, welche Services zentral für den Geschäftsbetrieb sind, welche Risiken bei deren Ausfall bestehen, welche Massnahmen notwendig sind und welche Abstriche akzeptiert werden können. Ohne Einschränkungen ist eine vollständige Abdeckung aller Services nicht umsetzbar.

Es ist notwendig, frühzeitig festzulegen, welche Services und Funktionalitäten unbedingt abgedeckt sein müssen und welche Einbussen in welchem Umfang toleriert werden können. Dies umfasst auch eine Einschätzung, wie schnell Ersatzlösungen verfügbar sein müssen und welche finanziellen sowie zeitlichen Ressourcen hierfür aufgewendet werden können.

Ein klarer Plan zur Organisation und Schulung des Personals – sowie des Change Managements insgesamt – ist essenziell, um die Einführung und Nutzung alternativer Lösungen effizient zu gestalten. Die Priorisierung der Services und die Festlegung von Massnahmen müssen dabei eng mit den Ergebnissen des Risikomanagements abgestimmt werden, um den Geschäftsbetrieb auch in Ausnahmesituationen aufrechtzuerhalten.

9.1 Identity Access Management

Problemstellung:

Das Identity Access Management (IAM) ist zentral für die Verwaltung von Zugängen zu Systemen und Tools. Diese zentrale Rolle führt dazu, dass bei einem Ausfall des IAM-Systems der Zugriff auf wichtige Anwendungen und Services beeinträchtigt wird, was weitreichende Folgen für den Betrieb haben kann.

Quintessenz:

Es gibt Massnahmen, die bereits umgesetzt werden können, um die Abhängigkeit von Active Directory (AD) zu reduzieren. Eine Option ist der Einsatz eines Meta-Directorys eines anderen Anbieters, welches die IAM-Funktionalitäten übernimmt und unabhängig von AD betrieben wird. Um die gesamte Abhängigkeit von AD zu eliminieren, müssen jedoch auch die übrigen Funktionen von AD mit Alternativen ersetzt werden, vgl. Kap. 9.9.

Nächste Schritte:

- Kantonsspezifische Architektur:
  Eine spezifische Ausgestaltung der Architektur auf kantonaler Ebene, die darauf abzielt, die Abhängigkeit vom Active Directory (AD) und Entra ID (Pendant von AD in der Microsoft-Cloud) zu minimieren, müsste sicherstellen, dass IAM-Services (Identity and Access Management) auch bei einem Ausfall von AD / Entra ID im Rahmen von IT-SCM-Szenarien weiterhin funktionsfähig bleiben.
- Analyse kritischer Services:
  Jede Organisationseinheit (OE) müsste dabei prüfen, welche ihrer Services kritisch sind, insbesondere solche, die über Single Sign-On (SSO) angebunden sind.

- Alternative Anmeldeverfahren:
  Für alle Services sollte in einem solchen Fall bewertet werden, ob alternative Anmeldeverfahren existieren, die bei einem Ausfall von SSO verwendet werden können. Diese Alternativen sollten dann auf ihre Praxistauglichkeit und Sicherheitsanforderungen geprüft werden.
- Strategieentwicklung:
  Basierend auf den Ergebnissen dieser Prüfungen sollte jede Institution eine klare Strategie entwickeln, um den Betrieb der kritischen Services auch bei Störungen sicherzustellen.

In einer Microsoft-Umgebung wird für das Identity Access Management (IAM) «Active Directory» (AD) und in der Microsoft Cloud Entra ID eingesetzt. AD ist ein Verzeichnisdienst, der in Windows-Netzwerken eine zentrale Rolle spielt. Nebst IAM wird AD auch eingesetzt, um Geräte und andere Netzwerkressourcen zentral zu verwalten.

Eine Alternative zu Entra ID gibt es nicht, beim Ausfall von Entra ID sind die Zugriffe auf Cloud-Services von Microsoft nicht möglich.

Grundsätzlich kann die Abhängigkeit von AD bzgl. der IAM-Funktionalität reduziert werden, indem ein anderes Produkt für ein sog. Metadirectory eingesetzt wird. Die Benutzer- und Gruppenverwaltung, Passwörter, Authentifizierung, Zugriffskontrolle und Berechtigungen würden dann in diesem separaten Metadirectory verwaltet, AD synchronisiert die notwendigen Daten. Ja nach Ausfallszenarium hätte dies dann unterschiedliche Auswirkungen:

- Meta-Directory fällt aus: AD kann mit den vorhandenen Daten weiterhin die IAM-Funktionen erfüllen, jedoch ohne Aktualisierung der Daten (z.B. aus Anpassungen von Berechtigungen oder Mutationen von Benutzern), damit diese Anpassungen beim Hochfahren des Meta-Directory nicht überschrieben werden.
- AD fällt aus: Die IAM-Services sind weiterhin verfügbar. Der Zugriff auf alle Anwendungen und Services, die unabhängig von AD sind, ist mittels Meta-Directory weiterhin möglich.

Solch eine Lösung kann jedoch nicht kurzfristig realisiert werden. Die Architektur der Betriebsumgebung müsste entsprechend konzipiert, geplant und umgesetzt werden, und die Betriebsumgebung müsste dauerhaft mit diesem alternativen Produkt betrieben werden. Dies würde zusätzliche Kosten für die Lizenzierung und den Betrieb dieses Zusatz-Services sowie eine Erhöhung der Komplexität der Gesamtarchitektur bedeuten. Zudem würde dies die bestehenden Abhängigkeiten um ein weiteres Produkt vergrössern.

Open Source Alternativen zur IAM-Funktion von Active Directory gibt es nur mit reduziertem Umfang. Beispiele:

- OpenLDAP ist eine OSS-Implementierung des LDAP-Protokolls, das einen offenen Verzeichnisdienst für die Verwaltung von Benutzerdaten, Gruppen und anderen Ressourcen bietet. Jedoch sind für eine vollständige Integration von OpenLDAP zusätzliche Tools und Erweiterungen notwendig, weil die Möglichkeiten zur Verwaltung von Computerobjekten oder Gruppenrichtlinien nicht so umfassend wie bei Active Directory sind.
- FreeIPA (Identity, Policy, and Audit) ist eine Open Source Lösung für Identitäts- und Zugriffsmanagement, die auf Linux- und Unix-Plattformen ausgerichtet ist. Sie basiert auf Technologien wie LDAP, Kerberos und DNS und beinhaltet viele der Funktionen von AD. Jedoch ist FreeIPA primär auf Linux/Unix-basierte Umgebungen ausgelegt. Die Integration in Windows-Umgebungen ist prinzipiell möglich, kann jedoch nicht so nahtlos implementiert werden wie bei Active Directory.

- Univention Corporate Server (UCS) inkl. Nubus ist eine Open Source IAM-Lösung auf Basis von LDAP, Kerberos und SAML. Sie ermöglicht die zentrale Verwaltung von Benutzern und Ressourcen, unterstützt hybride Cloud-Szenarien sowie die Integration in Linux- und Windows-Umgebungen. Allerdings deckt UCS den Funktionsumfang von Active Directory, insbesondere bei Gruppenrichtlinien, nicht vollständig ab.
- Andere Lösungen wie Red Hat Identity Management (idM) oder Okta sind auf spezifische Umgebungen ausgelegt (idM für Linux, Okta für Cloud-Identitätsmanagement). Sie sind als vollständige AD-Alternativen nur bedingt geeignet.
- Es wäre noch zu untersuchen, ob AGOV (das Behörden-Login der Schweiz) als vollständige IAM-Lösung innerhalb der öffentlichen Institutionen eingesetzt werden könnte.

Somit ist es theoretisch möglich, einen alternativen Service zu IAM einzusetzen. Ein kurzfristiges Hochfahren von solch einem Service ist jedoch nicht realistisch. Die Lösung müsste dauerhaft entweder als Klammer um AD (IAM) oder als Ersatz für AD betrieben werden.

9.2 Office-Anwendungen

Problemstellung:

Die Verfügbarkeit von Microsoft Office-Anwendungen ist in vielen Organisationen zentral für die Bearbeitung von Dokumenten. Ein Ausfall dieser Anwendungen kann zu erheblichen Einschränkungen im Arbeitsablauf führen. Teilweise werden Office-Funktionen auch in Fachanwendungen eingesetzt.

Quintessenz:

Alternativen zu Microsoft Office sind vorhanden, weisen jedoch Kompatibilitätsprobleme und Funktionalitätsdefizite auf. Im IT-SCM Szenario können die alternativen Produkte trotz Einschränkungen eingesetzt werden. Der rasche Ersatz der Office-Funktionen in Fachanwendungen ist jedoch nicht möglich. Im IT-SCM Szenario müsste auf die entsprechenden Funktionen in den Fachanwendungen oder sogar gänzlich auf den Einsatz dieser Fachanwendungen verzichtet werden. Bei neuen Releases des Microsoft-Angebots müsste stets geprüft werden, welche neuen Funktionen eingeführt werden sollen, um keine neuen Abhängigkeiten entstehen zu lassen.

Nächste Schritte:

- Einigung auf einen gemeinsamen offenen Dokumentenstandard aller öffentlichen Institutionen im Sinne eines eCH-Standards (z.B. Open Document Format)
- Prüfung von Alternativen zu Microsoft Office
- Einfache Gestaltung der eingesetzten Office-Vorlagen, damit sie auch in alternativen Office-Produkten eingesetzt werden können
- Weitgehender Verzicht auf komplexe Funktionen wie Makros in Dokumenten
- Prüfung der Möglichkeiten, Fachanwendungen ohne Office-Funktionalitäten einzusetzen
- Konfiguration von M365 so dass Dateien jeweils auch lokal auf den Clients gespeichert werden, um deren Verfügbarkeit auch im IT-SCM Szenario sicherzustellen

Sollten Microsoft Office-Anwendungen nicht mehr verfügbar sein, gibt es grundsätzlich mehrere Alternativen, mit denen Microsoft Office-Dateien (wie Word-, Excel- und PowerPoint-Dateien) bearbeitet werden können. Beispiele für Open Source Office-Suiten sind OnlyOffice, LibreOffice

und OpenOffice. Eine weitere Alternative ist auch Softmaker Office, vor allem aufgrund der guten Kompatibilität. Allerdings müsste diese Lösung lizenziert werden, da es sich nicht um Open Source Software handelt.

Alle Alternativen erfordern die Bereitstellung der Services auf einem Server. Somit müssten diese Services parallel zu Microsoft-Services dauerhaft betrieben werden, damit in einer IT-SCM Situation der Service für Office-Anwendungen rasch zur Verfügung gestellt werden kann.

Es gibt auch Alternativen, die keine Installation auf Server benötigen und in der Cloud verfügbar sind. Dazu zählen Open Source Lösungen, wie z.B. Collabora, OnlyOffice, und kommerzielle Services, wie z.B. Google Workspace, dessen Einsatz mit einem entsprechenden Benutzerkonto bei Google möglich ist. Für einen IT-SCM-Fall kann ein solcher kommerzieller Service von Google eine mögliche Option darstellen. Allerdings ist zu beachten, dass ein Wechsel zu einem anderen kommerziellen Service die gleichen Herausforderungen mit sich bringt wie der Einsatz von Microsoft-Services u.a. Datenschutz-Aspekte.

Bei allen Alternativen zu Microsoft Office Services gibt es jedoch Einschränkungen bei der Kompatibilität mit Microsoft-Dateien (meistens im Open XML Format). In der Regel können Microsoft-Dateien in den alternativen Produkten eingelesen und bearbeitet werden, jedoch ist die umgekehrte Richtung oft mit grösseren Problemen verbunden (v.a. bei Zusatzfunktionen wie Kommentaren, Nachverfolgung usw.). Bei komplexen Funktionen wie dem Einsatz von Makros und anspruchsvollen Formeln ist jedoch die Kompatibilität oft nicht mehr gegeben. Zudem muss überprüft werden, ob bestehende Dokumentvorlagen auch mit den alternativen Produkten weiterhin genutzt werden können.

In einem IT-SCM Fall ist es von zentraler Bedeutung, dass der Zugriff auf Dateien weiterhin gewährleistet ist. Dafür muss M365 so konfiguriert sein, dass die Dateien jeweils nicht nur in der Cloud, sondern auch auf den Clients gespeichert werden. Somit wäre in einem IT-SCM Fall grundsätzlich der Zugriff auf die lokalen Dateien und deren Bearbeitung in einem Web-Service möglich. Voraussetzung ist, dass der Client noch funktionsfähig und der Zugriff auf das Internet noch möglich ist.

Eine weitere Herausforderung stellt der Umgang von MS-Office-Funktionen in Fachanwendungen dar (z.B. Generieren von Dokumenten). Für das IT-SCM Szenario sind kurzfristige Massnahmen nicht möglich, weil Anpassungen in den entsprechenden Fachanwendungen implementiert werden müssten. Fallweise können die Fachanwendungen ohne MS-Office-Funktionen verwendet werden, ansonsten müsste auf den Einsatz dieser Fachanwendungen verzichtet werden.

9.3 Mail

Problemstellung:

Ein Ausfall des Microsoft-Mailservices beeinträchtigt nicht nur die E-Mail-Kommunikation, sondern auch die Kalender- und Kontaktverwaltung. Ohne Zugriff auf Kalender und Kontakte können keine Besprechungen geplant oder Termine koordiniert werden, was zu Verzögerungen und ineffizienten Arbeitsabläufen führt. In öffentlichen Organisationen würde dies die interne und externe Kommunikation erschweren und damit die Produktivität und das Vertrauen in die Organisation gefährden.

Quintessenz:

Bei einem Ausfall des Microsoft-Mailservices bestehen mehrere Möglichkeiten: Einsatz eines alternativen Mailservices und Nutzung lokaler Outlook-Daten für begrenzte Kommunikation, Betrieb eines parallelen Mailservices oder Mail-Mirroring.

Nächste Schritte:

- Detaillierte Bewertung der aufgeführten Varianten, unter Berücksichtigung von Themen wie Gruppenmails, Spam-Filter, Unterstützung von Labeling (z.B. vertraulich, öffentlich) und deren Behandlung, Integration von Fachanwendungen, Mail-Backbone-Infrastruktur.
- Prüfung inwiefern eine alternative Lösung ausschliesslich browserbasiert sein kann oder auch offline verfügbar sein muss, was eine Client-Installation erfordern würde.
- Detaillierte Prüfung der gewählten Lösungsvariante mit einer Pilotinstallation.

Bei einem Ausfall des Mailservices ist es möglich, einen alternativen Mailservice zu Microsoft einzusetzen. Grundsätzlich muss entschieden werden, ob der alternative Mailservice für alle oder nur für ausgewählte Benutzer bereitgestellt werden soll.

Für alternative Mailservices gibt es die folgenden Varianten:

Variante 1) Die einfachste Variante ist das **Bereitstellen von leeren Mail-Accounts** beim alternativen Mailprovider.

- Im IT-SCM Szenario müssen die eingehenden Mails auf den alternativen Mailprovider umgeleitet werden (die konkrete Lösung ist abhängig davon, wo der Mailbackbone betrieben wird, z.B. ein Umleitungs-Service von Swisscom).
- Für den Versand von Mails gibt es zwei Varianten:
  - Outlook-Client ist verfügbar und beinhaltet alle Mails, Adressen, Kalendereinträge usw. auf dem lokalen Client-Rechner, weil die Synchronisation mit der Cloud dauerhaft eingeschaltet war (Stand letzte Synchronisation vor dem Ausfall). In diesem Fall kann mit dem alternativen Mailservice von einem Drittanbieter gearbeitet werden. Die notwendigen Daten (z.B. Mailadressen) und die alte Korrespondenz ist zwar nur im lokalen Outlook-Client verfügbar. Diese können jedoch fallweise manuell verwendet werden, um Mailkorrespondenz aufrechtzuerhalten.
  - Outlook-Client ist nicht verfügbar oder beinhaltet keine Daten, weil sie jeweils nur in der Cloud gespeichert wurden. In diesem Fall kann auch auf einen alternativen Mailservice von einem Drittanbieter zurückgegriffen werden. Jedoch ist der Einsatz stark limitiert, wenn keine Adressdaten und keine Mail-Historie vorhanden sind. Falls die Benutzer lokal Archivkopien der Mails ablegen, könnten diese eingesetzt werden, um auf eine reduzierte Menge von Daten Zugriff zu haben.

Variante 2) Die zweite Variante ist das **Bereitstellen einer parallelen Mailumgebung bei einem alternativen Mailservice-Provider**. Die Mails werden bereits im Normalbetrieb an beide Adressen verschickt. Wichtig ist, dass auch der Inhalt vom Mail-Directory beim alternativen Mailservice verfügbar ist. Hinweise:

- Die Mails in der alternativen Umgebung wären dann alle im Eingangskorb ersichtlich. Die benutzerspezifisch eingerichtete Ordnerstruktur wird nicht übertragen.
- Diese zweite Mailumgebung müsste eine gewisse Kapazität haben (wie die Exchange-Produktionsumgebung), was mit entsprechenden Kosten verbunden wäre. Das regelmässige Löschen der Mails auf der alternativen Umgebung sollte zeitgesteuert

erfolgen (z.B. Löschen der Mails, die älter als 12 Monate sind), damit die notwendige Kapazität gesteuert werden kann.

Variante 3) Die dritte Variante ist ein **Mirroring-Service**, bei dem der gesamte Mailbox-Inhalt inkl. Ordnerstruktur und Maildirectory laufend auf eine Sekundärplattform mit einem spezifischen Tool (z.B. Quest) synchronisiert wird. Beim Ausfall des Mailservice können die Benutzer in dieser alternativen Umgebung wie üblich arbeiten. Auch Kalenderfunktionen der Benutzer wären verfügbar. Diese Lösung bietet für die Benutzer den grössten Komfort, jedoch sind die Ansprüche an die Betriebsorganisation und die Kosten sehr hoch. In einem IT-SCM Szenario muss die Replikation angehalten und die eingehenden Mails entsprechend umgeleitet werden. Für eine Rückkehr auf die Standard-Umgebung nach dem Abschluss des IT-SCM Zustandes muss die Migration sorgfältig geplant und geübt werden.

9.4 Datenablage und Kollaboration

Problemstellung:

Teams und SharePoint bieten einen grossen Funktionsumfang an, welche die Basis für die tägliche Zusammenarbeit in den meisten Institutionen bilden.

Quintessenz:

SharePoint-Ersatz für die Datenablage ist auch im IT-SCM Szenario möglich. Um die Daten auch lokal auf dem PC zur Verfügung zu haben, muss in SharePoint die Synchronisation aktiv sein, weil dann die Dateien automatisch lokal gespeichert werden und somit beim Ausfall von SharePoint vorhanden sind. Zudem sollten die im Notfall wichtigsten Daten (z.B. Krisenordner usw.) vorgängig auf einer alternativen Ablage vorgehalten und aktuell gehalten werden, damit diese im IT-SCM Szenario zentral verfügbar sind.

Für alle übrigen Funktionen von SharePoint (z.B. Workflow-Implementationen) sind kurzfristige Bereitstellungen von Open Source Lösungen nicht möglich.

Microsoft Teams kann kurzfristig mit einem alternativen Kollaborations-Service ersetzt werden, jedoch muss beachtet werden, dass die Chatverläufe und andere Daten nicht mehr vorhanden sind und auch nicht vom alternativen Service zurück in Teams geführt werden können.

Nächste Schritte:

- Prüfung, ob die Richtlinien der jeweiligen Organisation das Speichern lokaler Kopien von Daten auf den Clients erlauben.
- Bereitstellung IT-SCM relevanter Daten auf einer alternativen Ablage
- Sicherstellung der Zugriffe für entsprechende Benutzergruppen
- Test und Training der Umstellung von Teams auf einen alternativen Ablage- bzw. Collaborations-Service, damit dies in einer IT-SCM-Situation möglichst reibungslos funktioniert.

9.4.1 Datenablage in SharePoint

Um in einem IT-SCM-Szenario Zugriff auf die Dateien zu haben, muss in SharePoint die Option «Synchronisation» dauerhaft aktiv sein. Dadurch werden die Dokumente lokal auf Client-Rechner gespeichert und automatisch synchronisiert, d.h. jegliche Anpassungen in den Dateien (auch wenn sie offline ausgeführt werden) werden synchronisiert (sobald wieder online verfügbar). Dadurch wären die Dateien im IT-SCM-Szenario lokal auf den jeweiligen Rechnern verfügbar und könnten dort weiterbearbeitet werden. Vorgängig muss jedoch geprüft werden, ob die Richtlinien der Organisation das Speichern lokaler Kopien von Daten auf den Clients erlauben.

Der Austausch der Dateien mit anderen Benutzern kann beispielsweise per E-Mail erfolgen. Somit wäre zumindest ein sequenzielles Arbeiten mehrerer Personen an einer Datei möglich.

Grundsätzlich könnte der Austausch von Dateien mit anderen Benutzern und das gemeinsame Bearbeiten von Dokumenten auch auf einer alternativen Open Source Plattform erfolgen, falls eine solche Lösung im Kontext eines IT-SCM-Szenarios bereitgestellt wird (z.B. Nextcloud). Das gleichzeitige Bearbeiten der Dateien erfolgt in alternativen Office Lösungen wie Collabora oder OnlyOffice. Auch Nextcloud bietet die Synchronisation der Dateien auf lokale Rechner an. Sobald SharePoint wieder einsatzbereit ist, werden die Dateien, die in der Zwischenzeit angepasst wurden, automatisch synchronisiert. Die vollständige Kompatibilität dieser bearbeiteten Dokumente mit Microsoft Office ist jedoch nicht sichergestellt.

SharePoint ist auch in Teams als Datenablage integriert. Beim Ausfall von SharePoint ist diese Funktionalität von Teams nicht mehr gegeben.

Die im Notfall wichtigsten Daten (z.B. Krisenordner usw.) sollten vorgängig auf einer alternativen Ablage vorgehalten werden, damit diese im IT-SCM Szenario zentral verfügbar sind. Dabei ist es wichtig, dass (mittels organisatorischer und technischer Massnahmen) diese Daten aktuell gehalten werden.

9.4.2 Informationsbereitstellung und Kollaboration in SharePoint

SharePoint wird oft auch für die Bereitstellung von Informationen auf entsprechenden Websites (insbesondere für die Implementation von Intranet) verwendet. Im Rahmen von Projekten wird SharePoint auch für die Kollaboration eingesetzt (z.B. Aufgabenmanagement). Eine weitere beliebte Anwendungsmöglichkeit ist Workflow-Automatisierung.

Grundsätzlich gibt es Open Source Plattformen wie Nextcloud, die einen ähnlichen Funktionsumfang anbieten. Die Bereitstellung der SharePoint-Umgebung in einer anderen Plattform in einem IT-SCM-Szenario ist jedoch nicht ohne weiteres möglich, da dies mit einem grösseren Migrationsaufwand verbunden ist.

9.5 Kommunikation (Chat, Audio-/ Video ohne Telefonie)

Teams wird unter anderem für die Kommunikation mittels Chats und Audio-/ Videoconferencing eingesetzt. Für die in Teams enthaltenen SharePoint-Funktionen gelten dieselben Aussagen, die im Kapitel 9.4 beschrieben wurden. In einem IT-SCM Szenario ist es grundsätzlich möglich, für Benutzer kurzfristig Open Source Alternativen einzusetzen (z.B. Matrix, Jitsi Meet, Rocket.Chat). Sie bieten nicht den gesamten Funktionsumfang von Teams an, aber im IT-SCM Szenario sind sie ausreichend.

Ein Export der Chatverläufe aus Teams ist zwar möglich, aber ein Import in die alternativen Plattformen ist nicht möglich.

Konferenzräume, welche mit einer eigenen Teams-Identität ausgestattet sind, müssen manuell umkonfiguriert werden, was in einer IT-SCM Situation wohl nicht in Frage kommt.

9.5.1 Kurzfristiger Einsatz eines Kommunikationsservices

Bei einem Ausfall von Microsoft Teams ist es möglich, einen alternativen Kommunikationsservice auf Open Source Basis kurzfristig einzusetzen. Diese Alternativen bieten jedoch erhebliche Einschränkungen und stellen keine vollwertigen Ersatzlösungen dar (z.B. wegen fehlender Integration ins IAM-System). Die Varianten für den kurzfristigen Einsatz sind wie folgt:

- **Microsoft Teams-Client ist verfügbar und enthält Chatverläufe sowie Konfigurationsdaten lokal auf dem Endgerät.**
  In diesem Fall kann auf eine Open Source Lösung wie **Big Blue Bottom**, **Matrix** oder **Jitsi Meet** zurückgegriffen werden, um die Kommunikation via Chat und Videoanrufen aufrechtzuerhalten. Die alten Chatverläufe und Konversationen bleiben zwar nur im Teams-Client verfügbar und können nicht in die alternative Lösung migriert werden. Nutzer können jedoch fallweise manuell Informationen aus Teams abrufen und in die neue Kommunikationslösung übertragen.
  Diese Variante funktioniert für die Aufrechterhaltung von Echtzeitkommunikation. Allerdings ist die Integration mit bestehenden Microsoft-Services (z. B. SharePoint) und die Weiterführung von Konversationen aus Microsoft Teams nicht möglich. Zusätzlich muss für Videoanrufe und Gruppenkommunikation eine neue Umgebung mit separaten Links und Einstellungen eingerichtet werden.
  Nach Beendigung der IT-SCM-Situation müssten alle Konversationen wieder in Microsoft Teams integriert werden, was manuell nur eingeschränkt möglich ist. Dadurch ist diese Variante in der Praxis mit vielen Nachteilen verbunden.
- **Microsoft Teams-Client ist nicht verfügbar oder enthält keine gespeicherten Daten.**
  In diesem Fall kann ebenfalls auf eine alternative Lösung wie **Big Blue Button**, **Matrix** oder **Jitsi Meet** zurückgegriffen werden. Ohne gespeicherte Chatverläufe oder Konfigurationsdaten ist der Einsatz jedoch stark limitiert. Nutzer können zwar neue Konversationen und Videoanrufe über die alternative Plattform initiieren, jedoch fehlen historische Daten, bestehende Gruppenstrukturen sowie Kontaktlisten.
  Falls Benutzer lokal Notizen oder Dokumente mit wichtigen Kommunikationsinformationen gespeichert haben, können diese genutzt werden, um den Übergang zu erleichtern. Die alternative Lösung bleibt dennoch auf eine reduzierte Funktionalität beschränkt, da weder die bestehende Infrastruktur noch die Kontakte aus der Microsoft-Umgebung vollständig genutzt werden können.

Beide Varianten ermöglichen die temporäre Aufrechterhaltung der Kommunikation, sind jedoch ausserhalb der reinen Kommunikation via Audio und Video mit Einschränkungen verbunden. Der Verlust von Chatverläufen und die fehlende Integration in bestehende Systeme stellen gewisse Herausforderungen dar. Eine Rückkehr zur Microsoft-Umgebung nach Beendigung der IT-SCM-Situation erfordert zudem manuellen Aufwand, falls die Nachvollziehbarkeit der Kommunikation in der ursprünglichen Umgebung notwendig sein sollte.

9.5.2 Parallelbetrieb eines Kommunikationsservices

Ein Parallelbetrieb einer Unified Communications-Lösung kann Vorteile bieten, beispielsweise für verschiedene Einsatzszenarien oder Vertraulichkeitsstufen. Es gibt mehrere effiziente Alternativen zu Microsoft Teams, die schnell implementiert werden können, vor allem wenn auf eine vollständige Integration und Chatverläufe verzichtet werden kann. Andere Anbieter für Videomeetings oder alternative Kommunikationskanäle lassen sich ebenso effektiv nutzen.

Ein Parallelbetrieb muss geprüft werden, weil dies mit gewissen administrativen Aufwänden verbunden ist, unter anderem:

- Die gleichzeitige Konfiguration und Wartung von zwei Systemen.
- Die Verwaltung von zwei Benutzerprofilen und Berechtigungsstrukturen, was zu inkonsistenten Zugriffsrechten und potenziellen Sicherheitslücken führen kann.
- Die technische Herausforderung, eine zuverlässige Synchronisation und Migration von Daten (wie Nachrichten und Anrufprotokolle) sicherzustellen, falls nötig und gewünscht.

Zudem müssen die Mitarbeiter ein zusätzliches Kommunikationstool beherrschen und für das zweite System fallen zusätzliche, laufende Lizenzkosten an.

9.6 Telefonie mit Teams

Problemstellung:

Die Zuverlässigkeit der telefonischen Erreichbarkeit steht vor Herausforderungen, insbesondere im Hinblick auf mögliche Ausfälle der Festnetz- und zentralen Telefoninfrastruktur. Dies betrifft die interne Kommunikation sowie die externe Erreichbarkeit für Partner und Kunden. Es gilt, Ausfallszenarien vorzubereiten und alternative Kommunikationswege zu etablieren.

Quintessenz:

Die Kommunikationsinfrastruktur muss so gestaltet werden, dass auch bei Ausfällen von Festnetz oder zentralen Telefonlösungen die Erreichbarkeit aller relevanten Stellen und Personen gewährleistet ist. Dafür sind Diensthandys, IP-Telefonie sowie redundante Lösungen notwendig.

Nächste Schritte:

- Prüfung der Ausstattung mit Diensthandys:
  Es ist zu evaluieren, welche Mitarbeitenden bereits über ein Diensthandy verfügen und welche zusätzlich mit einem Diensthandy ausgestattet werden sollten, um eine zuverlässige Erreichbarkeit sicherzustellen.
- Einsatz von IP-Telefonen:
  Es ist zu prüfen, inwiefern IP-Telefone als Alternative eingesetzt werden können, um die Erreichbarkeit der Hauptrufnummern der Organisation aufrechtzuerhalten.
- Aufbau redundanter Infrastrukturen:
  Eine Analyse ist erforderlich, ob und wie eine redundante Infrastruktur parallel betrieben werden kann, um im Falle eines Ausfalls eine unterbrechungsfreie Kommunikation zu gewährleisten.

Die in diesem Kapitel aufgeführten Gedanken gehen davon aus, dass die Verwaltung mit einer Telefonie-integrierten Teams-Instanz arbeitet, d.h. die meisten Benutzer nutzen eine Festnetznummer und erhalten die entsprechenden Anrufe in Teams, aber für die Hauptnummer und Call-Center usw. wird eine separate Telefonzentrale betrieben. Weiter wird davon ausgegangen, dass das Routing der Telefonanrufe zu dieser Telefonzentrale, einem Call-Center oder Teams von einem Telefonie-Provider (z.B. Swisscom) gemacht wird und die Anrufe nicht direkt bei Microsoft ankommen.

Um die Kontinuität der Kommunikationsfähigkeit sicherzustellen, ist es essenziell, für verschiedene Szenarien eines Telefonausfalls Alternativen bereitzuhalten. Die folgenden Massnahmen bieten eine strukturierte Übersicht zu den Handlungsmöglichkeiten in drei wesentlichen Bereichen der Telefonie: Festnetznummern, Hauptrufnummer und Telefonzentrale.

9.6.1 Alternativen für Anrufe auf Festnetznummer

Der Service des erwähnten Telefonie-Providers kann so konfiguriert werden, dass bei Nichterreichbarkeit einer bestimmten Festnetznummer eine alternative Nummer angewählt wird.

- **Umleitung auf Mobiltelefone:**
  Alle Mitarbeitenden, die über Diensthandys verfügen, können über eine solche zentrale Umleitung der Festnetznummern auf ihre Mobiltelefone weiterhin erreichbar bleiben. Dies erfordert, dass eine Umleitung schnell und automatisiert eingerichtet werden kann oder bereits im Normalbetrieb genutzt wird. Ein Rückruf vom Diensthandy würde allerdings nicht mehr mit der Festnetznummer assoziiert.
- **Nutzung von Audio-/Videoconferencing-Lösungen:**
  Lösungen wie **Matrix**, **Zoom**, **Webex** oder **Jitsi Meet** können mit zusätzlichen Lizenzkosten so ausgestattet werden, dass sie über das öffentliche Telefonienetz erreichbar sind, entweder über die bestehenden Festnetznummern oder anderen, beliebigen Nummern. Im letzteren Fall wäre bei einem Rückruf die Nutzung der ursprünglichen Festnetznummer nicht mehr möglich.

9.6.2 Alternativen für die Hauptrufnummer (zentrale Erreichbarkeit)

In der oben beschriebenen Ausgangslage wird die Hauptnummer von einer Telefonzentrale betrieben, welche nicht über Teams läuft und daher von einem Microsoft-Ausfall nicht betroffen wäre. Nichtsdestotrotz wäre ein internes Weiterleiten der Anrufe nur unter erschwerten Bedingungen möglich, da ein Plattformbruch zwischen Hauptnummer und Mitarbeiternummer besteht.

- **Einsatz von IP-Telefonen** oder IP-Softphones (PC-basierte Telefonie-App)**:**
  Wenn die Festnetz-Infrastruktur ausfällt, können IP-Telefone mit einer internetbasierten Verbindung eingerichtet werden, um die Erreichbarkeit der Hauptrufnummer sicherzustellen. Diese Geräte sollten redundant mit separaten Netzwerken verbunden sein, um eine hohe Verfügbarkeit zu gewährleisten.
- **Fallback-Lösung auf Mobilgeräte:**
  Durch Weiterleitung der Hauptrufnummer auf eine zentrale Mobilfunknummer oder eine Reihe von Mobilgeräten kann die Erreichbarkeit der Organisation weiterhin sichergestellt werden.

9.6.3 Alternativen für die Telefonzentrale (Call Center)

Für Telefonzentralen (Call Center) gibt es im wesentlichen zwei Alternativen:

- **Unabhängige Lösungen für kritische Organisationen (z. B. Blaulicht-Organisationen):** Für Organisationen mit hohen Sicherheits- und Verfügbarkeitsanforderungen gibt es bewährte, von Microsoft unabhängige Produkte. Beispiele sind spezialisierte Kommunikationssysteme wie **Tetrapol** oder **TETRA**, die auch bei einem kompletten Internetausfall funktionsfähig bleiben.
- **Einsatz von Open Source Lösungen:** Open Source Plattformen wie **Asterisk** bieten flexible, und individuell anpassbare Alternativen für eine zentrale Telefonie-Infrastruktur. Diese können auf redundanten Servern betrieben werden, um die Ausfallsicherheit zu erhöhen.

9.7 Betriebssystem auf Clients

Problemstellung:

Ein Ausfall des Betriebssystems auf den Clients führt zu einem Verlust der Arbeitsfähigkeit auf den Client-Rechnern.

Quintessenz:

Kurzfristige Lösungen wie "Bring-your-own"-Clients oder die Bereitstellung von parallelen Clients mit alternativen Betriebssystemen (z.B. Linux) oder der Einsatz von mobilen Geräten mit iOS oder Android können als Notfalloptionen dienen. Diese erfordern jedoch detaillierte Planung und könnten bei einer hohen Anzahl von Nutzern an ihre Grenzen stossen. Der Ausfall des Betriebssystems macht einen raschen Ersatz oder die Nutzung von Cloud-Desktop-Lösungen erforderlich, um die Arbeitsfähigkeit schnellstmöglich wiederherzustellen.

Nächste Schritte:

Detaillierte Planung und Test von möglichen Lösungen: Cloud-Desktop, Bereitstellung von vorinstallierten Clients mit einem alternativen Betriebssystem wie z.B. Linux. Zudem umfassende Tests der Peripheriegeräte wie Drucker, Scanner und Card-Reader sowie die Einrichtung zentraler Services für Druck- und Scanlösungen unter Berücksichtigung von Sicherheits- und Datenschutzanforderungen.

9.7.1 Kurzfristige Lösungen

In einer Krisensituation ist ein Ausrollen von Ersatz-PCs in grossen Stückzahlen nicht realistisch. Deshalb bietet sich beim Ausfall des Microsoft-Betriebssystems auf den Clients die Möglichkeit an, auf Cloud-Desktop-Lösungen (VDI, siehe Kap. 9.8.3) zuzugreifen (z.B. von privaten Bring-your-own Geräten). Diese erlauben den Zugriff auf ein vollständig virtuelles Betriebssystem über den Browser- oder Citrix-artigen Protokollen. Es gibt keine „Cloud-basierten Betriebssysteme“ im traditionellen Sinne, die als vollständige Open Source Betriebssysteme in der Cloud eingesetzt werden können. Vielmehr handelt es sich um Cloud-Plattformen (wie OpenStack, OpenNebula und Cloud-init) und Container- und Virtualisierungs-Technologien (wie Docker, Kubernetes und CoreOS), die Cloud-Infrastrukturen ermöglichen und optimieren.

Solch ein Einsatz müsste jedoch im Voraus detaillierter ausgearbeitet und vertraglich geregelt werden. Insbesondere bei einer grossen Zahl von Benutzern, die gleichzeitig auf eine Cloud-Desktop-Lösung zugreifen, kann dies zu Skalierungsproblemen beim Service Provider führen.

Neben der reinen Desktop-Lösung wären die Integration und Nutzung von Peripheriegeräten wie Druckern, Scannern und Card-Readern essenziell, um die Arbeitsfähigkeit vollständig sicherzustellen. Diese Geräte müssten entweder über standardisierte Schnittstellen wie USB, Netzwerkprotokolle (z. B. IPP für Drucker) oder Remote-Desktop-Protokolle eingebunden werden. Für einige Anwendungen, wie etwa sichere Authentifizierungsverfahren über Smartcards, ist die nahtlose Funktion von Card-Readern unerlässlich.

9.7.2 Bereitstellen Clients mit alternativem Betriebssystem

Grundsätzlich wäre es denkbar, eine gewisse Anzahl von Clients mit einem alternativen Betriebssystem dauerhaft und parallel zur Microsoft-Umgebung bereitzustellen, z.B. Linux (kann insbesondere auch auf älteren Rechnern bereitgestellt werden, weil Linux wenig Ressourcen beansprucht). Android-Geräte wären ebenfalls eine denkbare Variante, auch wenn nur mit eingeschränktem Funktionsumfang. Bei einem vollständigen Ausfall vom Microsoft-Betriebssystem würden diese zum Einsatz kommen. Denkbar wäre auch eine Installation mit virtuellen Windows PCs, dies für den Fall, dass nur die eigene Infrastruktur nicht läuft. In beiden Varianten müsste eine entsprechende Anzahl von Rechnern jeweils vorinstalliert sein und die Konfiguration müsste aktuell gehalten werden. Solch eine Lösung wäre ressourcenintensiv und nur für eine kleine Anzahl von Benutzern mit beschränkter Funktionalität denkbar. Verschiedene Cloud-Anbieter offerieren skalierbare Modelle, in denen bei Bedarf die Kapazität rasch erhöht werden kann. Wieviel diese Versprechen wert sind, wenn alle Kunden bzw. eine grosse Anzahl von Benutzern gleichzeitig betroffen sind, sei allerdings dahingestellt.

9.8 Fernzugriff/ Remote Working Lösungen

Problemstellung:

Die Möglichkeiten für Fernzugriff und Remote Working erleichtern die Fernwartung von Systemen, Fernunterstützung von Benutzern sowie Remote Arbeiten für Mitarbeitende. Ein Ausfall dieser Lösungen bedeutet insbesondere Verlust an Produktivität und Flexibilität.

Quintessenz:

Es gibt sowohl kommerzielle als auch Open Source Alternativen zu den entsprechenden Microsoft-Services. Deren kurzfristige Aufschaltung ist jedoch mit erheblichem Aufwand verbunden. Ein Parallelbetrieb ist ebenfalls nicht zielführend.

Nächste Schritte:

Auf Basis einer Anforderungsanalyse den Einsatz von alternativen Lösungen (Open Source oder kommerzielle Produkte) prüfen.

9.8.1 Remote Access Service

Microsoft Remote Desktop ermöglicht den Zugriff auf einen entfernten Rechner oder eine virtuelle Maschine über das Internet. Damit kann auf Anwendungen und Dateien zugegriffen

und Netzwerkressourcen genutzt werden. In der Regel wird dies für die Fehlersuche und Problembehebung per Fernzugriff eingesetzt. Es basiert auf dem Open Source Anzeigeprotokoll «Remote Desktop Protocol» (RDP), das von Microsoft entwickelt wurde. Da es sich bei RDP um ein öffentlich dokumentiertes Protokoll handelt, ist es seit langem ein Ziel für Hacker, die mehrere Sicherheitslücken im Protokoll gefunden und ausgenutzt haben. In der Zwischenzeit sind mehrere RDP-Alternativen auf dem Markt erschienen – sowohl kommerzielle (z.B. TeamViewer, AnyDesk) als auch Open Source Lösungen (z.B. NoMachine), von denen viele je nach spezifischen Bedürfnissen viel mehr Möglichkeiten bieten.

Wenn es darum geht, die Abhängigkeit von Microsoft Remote Desktop zu reduzieren, kann eine dieser alternativen Lösungen eingesetzt werden.

9.8.2 Virtual Private Network (VPN)

Ein VPN erstellt eine verschlüsselte Verbindung (Tunnel) zwischen dem Gerät des Benutzers und dem Unternehmensnetzwerk über das öffentliche Internet. VPNs ermöglichen es daher Mitarbeitenden, sicher auf das Unternehmensnetzwerk zuzugreifen. Es gibt zu Microsoft VPN-Lösungen mehrere Open Source Alternativen, wie z.B. OpenVPN, WireGuard, SoftEther VPN, Pritunl (basiert auf OpenVPN und WireGuard), oder StrongSwan.

Diese alternativen Lösungen können eingesetzt werden, um die Abhängigkeit von Microsoft zu reduzieren. Ein kurzfristiger Wechsel auf eine dieser Lösungen ist nicht möglich, sowohl aus administrativen Gründen (Einrichten der Benutzerprofile, Organisation der notwendigen Zertifikate, Kommunikation und Benutzerschulung zur neuen Lösung, usw.) als auch aufgrund möglicher technischer Herausforderungen (Kompatibilität mit der bestehenden Infrastruktur).

9.8.3 Virtual Desktop Infrastructure (VDI)

VDI hostet Desktop-Umgebungen auf zentralen Servern. Benutzer greifen über das Internet auf diese virtuellen Desktops zu, die auf einem zentralen Server laufen. Somit kann für alle Benutzer eine einheitliche Desktop-Umgebung bereitgestellt werden. Microsoft bietet dazu die «Azure Virtual Desktop» an.

Es gibt mehrere Open Source Alternativen zu den Microsoft VPN-Lösungen, wie beispielsweise Promox VE, XCP-ng (basiert auf dem Citrix XenServer), Apache CloudStack. Alle diese Lösungen haben jedoch verschiedene Einschränkungen hinsichtlich des Funktionsumfangs im Vergleich zu spezialisierten, kommerziellen VDI-Lösungen. Soll die Abhängigkeit von Microsoft reduziert werden, müssten deshalb eher kommerzielle VDI-Lösungen in Betracht gezogen werden, wie z.B. Citrix oder VMware.

9.9 System Management

In der Microsoft-Umgebung erfolgt das System Management, z. B. die Verwaltung der Clients und Server mit Active Directory (AD) sowie Intune.

On-Premises-Variante: Soll die Abhängigkeit von Microsoft reduziert bzw. eliminiert werden, könnte ein gänzlich anderes Produkt eingesetzt werden, z.B. Univention Corporate Server (UCS), ein Server-Betriebssystem mit integriertem Identity- und Infrastrukturmanagementsystem für die zentrale und plattformübergreifende Verwaltung von Servern, Services, Clients, Desktops und

Benutzern sowie von unter UCS betriebenen virtualisierten Computern. Andere On-Premises Open Source Alternativen wie Samba oder FleetDM kommen jedoch eher für kleinere Organisationen in Frage.

Cloud-Variante: Für das Management von Patches und Updates der Clients wird Intune (eine Microsoft Cloud-Lösung) eingesetzt. Als mögliche Open Source Alternativen könnten cloudbasierte Tools wie SaltStack, Ansible oder Puppet untersucht werden.

Inwieweit diese Open Source Alternativen für das System Management – sowohl On-Premises als auch Cloud-basiert – eingesetzt werden können, müsste noch geprüft werden. Ihr kurzfristiger Einsatz in einem IT-SCM-Szenario ist jedoch nicht realistisch. Ein paralleler Betrieb verschiedener Lösungen ist mit hohen Risiken verbunden, da bei korrupten Systemen die Funktionsfähigkeit der Clients beeinträchtigt werden könnte oder die beiden Management-Systeme sich gegenseitig behindern könnten. Fehler bei System-Management-Tools, ob On-Premises oder Cloud-basiert, können gravierende Konsequenzen haben, wie z. B. die Notwendigkeit, sämtliche Clients neu aufzusetzen.

9.10 Mobile Device Management (MDM)

Problemstellung:

Bei einem Ausfall des MDM-Systems können mobile Geräte nicht mehr effektiv verwaltet werden. Wichtige Sicherheitsfunktionen wie das Fernsperren oder Löschen von Geräten im Fall von Verlust oder Diebstahl fallen weg. Darüber hinaus können Sicherheitsrichtlinien nicht mehr auf mobilen Geräten durchgesetzt werden, was erhebliche Sicherheitsrisiken mit sich bringt.

Quintessenz:

Kommerzielle wie auch Open Source Alternativen zu Microsoft MDM sind grundsätzlich verfügbar. Sie weisen aber im Vergleich zu Microsoft begrenzte Funktionen und Skalierbarkeit auf. Insbesondere die Sicherstellung der Informationssicherheit der Daten, d.h. Durchsetzen der Regeln gemäss Klassifikation der Dateien (vertraulich, intern usw.) auf den mobilen Geräten kann bei den alternativen Services nicht vollumfänglich integriert sichergestellt werden.

Nächste Schritte:

Fortführung der Marktbeobachtung, bis Alternativen für MDM verfügbar sind.

Ein MDM-Ausfall von wenigen Tagen kann erhebliche Sicherheits- und Produktivitätsprobleme verursachen. Um die Risiken zu minimieren, sind Notfallpläne, alternative Sicherheitsvorkehrungen und eine schnelle Wiederherstellung des Systems entscheidend.

Die wichtigsten Konsequenzen sind Sicherheitsrisiken wie z.B.

- Ohne MDM können verlorene oder gestohlene Geräte nicht aus der Ferne gesperrt oder gelöscht werden
- Mitarbeiter können unter Umständen beliebige Apps installieren, die möglicherweise nicht den Sicherheitsrichtlinien entsprechen. Ungesicherte Apps oder Dateien können herunterladen werden, was zu Malware-Infektionen führen kann

- Ohne MDM ist es schwierig sicherzustellen, dass alle Geräte und Daten verschlüsselt sind
- Geräte können sich mit unsicheren WLAN-Netzwerken verbinden, wodurch Angriffe erleichtert werden

Grundsätzlich gibt es kommerzielle Alternativen (z.B. Citrix) und auch Open Source Alternativen zur MDM-Lösung von Microsoft (Intune). Die Open Source Alternativen sind eher für kleinere Organisationen geeignet. Sie decken nicht alle Funktionen ab, insbesondere die Sicherstellung der Informationssicherheit der Daten. Die Lösung von Microsoft kann sicherstellen, dass die Regeln gemäss Klassifikation der Dateien (vertraulich, intern usw.) auch auf den mobilen Geräten durchgesetzt werden können, was bei den alternativen Services nicht vollumfänglich integriert sichergestellt werden kann.

Zudem ist der parallele Betrieb von alternativen MDM-Services nicht möglich, da Mobile Devices nur mit einem einzigen Service gesteuert werden können. Als Vorbereitung für einen Ausfall vom Microsoft MDM-Service könnte eine neue Lösung vorbereitet und aufgesetzt werden. In einem IT-SCM Vorfall müsste das rasche Umschalten auf die alternative Lösung mit Hilfe der Benutzer durchgeführt werden. Während der Umkonfigurierung ist das Gerät ungeschützt, d.h. der Benutzer könnte beliebige Apps installieren oder schützenswerte Daten mit nicht-autorisierten Personen teilen.

10 Open Source Alternativen zu Microsoft für Exit-Strategie

Fragestellung: Welche Schritte können oder sollten bereits heute einleitet werden, um sich auf ein potenzielles Vertragsende vorzubereiten – sei es durch eine eigene Kündigung oder durch eine Kündigung seitens Microsoft?

Die Frage lässt sich vorab durch eine Marktanalyse beantworten: **Eine vollständige 1:1-Alternative zu Microsoft existiert nicht.** Jede verfügbare Lösung erfordert Kompromisse, sowie eine Anpassung an die bestehende IT-Architektur. Daher würde ein geplanter Ausstieg aus dem Microsoft-Ökosystem eine strategische und politische Entscheidung erfordern und wäre für eine einzelne öffentliche Verwaltung an sich nur sehr schwer umsetzbar.

Grundsätzlich sind jedoch die in Kapitel 9 aufgeführten IT-SCM Massnahmen auch als Vorbereitung für ein Vertragsende mit Microsoft geeignet.

Weitere Herausforderungen sind:

- Die Bereitstellung alternativer Services zu Microsoft, sowie ein Wechsel sind äusserst aufwendig, zeit- und ressourcenintensiv. Um einen reibungslosen Übergang sicherzustellen, müssten alternative Lösungen im Detail konzipiert, durch «Proof of Concept»-Installationen getestet und in den meisten Fällen parallel zur bestehenden Microsoft-Infrastruktur aufgebaut werden. Ein isoliertes Vorgehen einzelner öffentlicher Institutionen ist in der aktuellen Situation, die durch das Fehlen interkantonaler Standards (eCH) und geeigneter Anbieter geprägt ist, mit erheblichen Risiken verbunden. Ein geplanter Ausstieg sollte daher idealerweise unter der Koordination einer zentralen Stelle (z. B. DVS oder eOperations) erfolgen, um die Voraussetzungen (eCH-Standards, etc.) für eine erfolgreiche Umsetzung zu schaffen.
- Bei einem vollständigen Verzicht auf Microsoft Services müssten alle Fachanwendungen vollständig von Microsoft-Services bereinigt werden (z.B. Bearbeiten oder Generieren von Office-Dokumenten aus den Fachanwendungen). Diese Arbeiten und die damit verbundenen Aufwände müssten die Institutionen selbst tragen, weil die Fachanwendungen in der Regel recht spezifisch ausgelegt sind. Die Migration von Fachanwendungen, die auf spezifischer Standard-Software basieren und in mehreren Kantonen eingesetzt werden, sollten dann allerdings durch koordinierte Ansätze (z.B. gemeinsame, zentrale Verhandlungen mit Anbietern von Fachanwendungen) angegangen werden.
- Die beschaffungsrechtlichen Aspekte sind zu berücksichtigen, sowohl bei einem allfälligen Alleingang einer Institution als auch bei einer gemeinsamen Lösung. Eine koordinierte Vorgehensweise kann dazu beitragen, einheitliche Lösungen zu erreichen und Doppelspurigkeiten zu minimieren. Gemeinsame Beschaffungsvorhaben können zudem zu besseren Verhandlungsposition gegenüber Anbietern führen.
- Die betrieblichen Aspekte sind die elementarsten Risiken. Aktuell sind die Anbieter von Open Source Lösungen eher kleinere Firmen. Wenn in kurzer Zeit alle Kantone oder sogar alle öffentlichen Institutionen der Schweiz die Leistungen bei derselben Firma beziehen, wird sie voraussichtlich nicht in der Lage sein, in kurzer Zeit die Service-Kapazitäten entsprechend auszubauen. Zudem birgt das Vorgehen auch das Risiko, von einer kleinen Firma abhängig zu sein. Ein neuer Ansatz ist daher notwendig, um diese Herausforderungen zu bewältigen. Eine mögliche Variante wäre die Entwicklung und Nutzung einer Behördenleistung wie beispielsweise der Swiss Government Cloud (SGC), ergänzt durch einen Multi-Provider-Ansatz. Dies würde sicherstellen, dass die Abhängigkeit nicht lediglich auf einen neuen Anbieter

verlagert wird. Alternativ könnte eine Lösung mit einer grossen Firma verfolgt werden, die über ausreichendes Kundenpotenzial verfügt und mit einer Staatsgarantie ausgestattet ist, um Stabilität und langfristige Verlässlichkeit zu gewährleisten.

Fazit: Die Bereitstellung von alternativen Services zu Microsoft und ein Wechsel sind äusserst aufwendig, zeit- und ressourcenintensiv. Ein isolierter Alleingang einzelner öffentlicher Institutionen ist in der Regel aufgrund der Komplexität und der finanziellen und organisatorischen Herausforderungen kaum umsetzbar.

Die Erkenntnisse der Studie verdeutlichen, dass einzelne Verwaltungen kaum in der Lage sein werden, allein tragfähige Lösungen für die beschriebenen Herausforderungen zu entwickeln. Die Komplexität der technischen, organisatorischen und rechtlichen Anforderungen erfordert eine enge Zusammenarbeit. Ein Zusammenschluss der Akteure – idealerweise auf nationaler und sogar überstaatlicher Ebene, beispielsweise in Zusammenarbeit mit der EU – ist entscheidend, um Synergien zu schaffen, Standards zu entwickeln und Ressourcen effizient zu nutzen. Nur durch eine koordinierte, übergreifende Herangehensweise können langfristig nachhaltige und souveräne Lösungen realisiert werden.

Anhang

[1] Anhang A: Anforderungsanalyse, Marktanalyse, Interview mit öffentlichen Verwaltungen und Umfrage mit den Anbieterfirmen *(Excel-Dokument, online gut lesbar)*

Beilagen

[B1] Studie zu Open Source Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung: *Backend-Services;* Berner Fachhochschule; Version 1.8 vom Februar 2024

[B2] Studie zu Open Source Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung: *Frontend-Services (Client-Anwendungen)*; Berner Fachhochschule; Version 1.0 vom Februar 2024

[B3] Die Open Innovation und Open Source Strategie des Landes Schleswig-Holstein; Staatskanzlei; Version 1.0 vom 20.11.2024

Glossar

Begriff	Beschreibung / Erläuterung
Active Directory (AD)	Verzeichnisdienst von Microsoft zur zentralen Verwaltung von Benutzern, Gruppen, Computern und anderen Ressourcen innerhalb eines Netzwerks.
Business Continuity Management (BCM)	Strategien und Massnahmen zur Sicherstellung der Geschäftsfortführung im Falle von Notfällen oder Krisen.
Cloud Governance	Richtlinien und Prozesse zur Steuerung, Verwaltung und Kontrolle von Cloud-Services innerhalb einer Organisation.
Copilot (Microsoft)	KI-gestützte Assistenzfunktion, die in Microsoft-Services integriert ist und Benutzer bei verschiedenen Aufgaben unterstützt.
Digitale Souveränität	Die Fähigkeit von Organisationen oder Staaten, ihre digitalen Infrastrukturen und Daten unabhängig und selbstbestimmt zu kontrollieren.
Digitale Verwaltung Schweiz (DVS)	Zusammenarbeitsorganisation für die strategische Steuerung und Koordination der Digitalisierungsaktivitäten von Bund, Kantonen und Gemeinden https://www.digitale-verwaltung-schweiz.ch/
eCH-Standards	Standards im Bereich E-Government, die vom Verein eCH (https://www.ech.ch/de) gefördert, entwickelt und verabschiedet werden. Diese Standards dienen der effizienten elektronischen Zusammenarbeit zwischen Behörden, Unternehmen und Privaten.

Begriff	Beschreibung / Erläuterung
eOperations Schweiz	Gemeinsame Organisation von Bund, Kantonen und Gemeinden für den Betrieb, die Beschaffung und die Weiterentwicklung digitaler Verwaltungsdienste.
Identity and Access Management (IAM)	Verwaltungssystem für digitale Identitäten und Zugriffsrechte innerhalb einer IT-Infrastruktur.
Interoperabilität	Die Fähigkeit unterschiedlicher Systeme, Organisationen oder Anwendungen, nahtlos zusammenzuarbeiten und Daten auszutauschen.
IT Service Continuity Management (IT-SCM)	Massnahmen zur Sicherstellung der Verfügbarkeit von IT-Services im Falle von Ausfällen oder Störungen.
Request for Information (RFI)	Vorgehen für die Gewinnung von Marktübersicht anhand von Informationsanfragen an potenzielle Anbieter/ Leistungserbringer
Microsoft 365 (M365)	Suite von Cloud-basierten Produktivitäts- und Kollaborationsanwendungen, einschliesslich Office, Teams, SharePoint und Exchange.
Mobile Device Management (MDM)	Software zur zentralen Verwaltung und Sicherung mobiler Endgeräte in Unternehmen oder öffentlichen Institutionen.
Office-Format	Standardisierte Dateiformate für Büroanwendungen, z. B. Microsoft Open XML (.docx, .xlsx, .pptx) und Open Document Format (ODF).
Open Document Format (ODF)	Ein freies und offenes Dokumentenformat, das als Alternative zu proprietären Formaten wie Microsofts Open XML dient. ODF wird u. a. von Open Source Office-Suiten wie LibreOffice, OpenOffice und OnlyOffice unterstützt und ist in der Schweiz als eCH-0031-Standard anerkannt.
Open Source Software (OSS)	Software, deren Quellcode öffentlich zugänglich ist und von der Community weiterentwickelt werden kann.
Swiss Government Cloud (SGC)	Mit der Swiss Government Cloud (SGC) soll eine neue, auf die Anforderungen und Bedürfnisse des Bundes zugeschnittene Cloud-Infrastruktur aufgebaut werden. Die Realisierung des Vorhabens ist für die Jahre 2025 bis 2032 angesetzt. https://www.bit.admin.ch/de/sgc-de
Total Cost of Ownership (TCO)	Gesamtkosten einer Investition über den gesamten Lebenszyklus, einschliesslich Anschaffung, Betrieb, Wartung und Entsorgung.
Virtual Desktop Infrastructure (VDI)	IT-Infrastruktur, die es Benutzern ermöglicht, von fast jedem Gerät aus auf Unternehmenscomputerressourcen zuzugreifen