Vortrag des Gemeinderats an den Stadtrat

Potenzialanalyse Open Source Software (POTOSS)

1. Management Summary

Mit SRB 2016-3870 vom 18. August 2016 erteilte der Stadtrat dem Gemeinderat den Auftrag, eine Potenzialanalyse in Bezug auf Open Source Software (OSS) zu machen und durch praxisbezogene Pilotprojekte die Machbarkeit einer Umstellung auf Open Source Produkte in der Stadtverwaltung Bern zu prüfen.

Mit diesem Auftrag starteten die Informatikdienste (ID) zusammen mit der in einer offenen Ausschreibung gewählten Firma Adfinis SyGroup AG das Projekt POTOSS. In fünf Pilotprojekten in den Bereichen Basis Client, Fachapplikationen, Groupware[1], Virtualisierung und CMI Axioma wurden in der Folge umfangreiche technische Tests durchgeführt und Schlussfolgerungen daraus gezogen. Die vorliegende Analyse zeigt auf, welche praktischen Untersuchungen für den Einsatz von OSS gemacht wurden, wo die Chancen und der Mehrwert von OSS in der Stadtverwaltung liegen, welche Risiken und Grenzen für einen Einsatz von OSS bestehen, wie der wirtschaftliche Vergleich von OSS mit proprietärer Software ausfällt und welche Empfehlungen daraus resultieren.

In der Informatik der Stadtverwaltung werden seit Jahren sowohl Open Source-Produkte als auch proprietäre Software-Produkte eingesetzt; sie ist in diesem Sinne ein klassischer Mischbetrieb. Über alle Produkte hinweg gelten dieselben Anforderungen: Sie müssen funktional, stabil und wirtschaftlich sein. Mit Blick auf diese Grundsätze an die Informatik der Stadtverwaltung zeigt die Potenzialanalyse auf, dass zum heutigen Zeitpunkt ein gänzlicher Umstieg auf OSS nicht zweckmässig wäre, da bei den Anforderungen Einschränkungen in Kauf genommen werden müssten. Die grösste Motivation, OSS-Produkte einzusetzen besteht darin, die Abhängigkeit von marktdominanten Herstellern zu lösen und sich deren Diktat der Lizenzmodelle und -kosten zu entziehen. Durch den Einsatz von OSS-Produkten fallen die Lizenzkosten weg; diese machen am Betrieb der IT-Infrastruktur der Stadtverwaltung rund 14 % aus. Diese Einsparung wird jedoch relativiert durch die notwendigen Supportverträge mit OSS-Fachleuten, den sogenannten Subscriptions. Zudem verhindern die hohen Investitionen, welche zum Aufbau der OSS-Plattformen, zum Wissensaufbau der Mitarbeitenden und zur Migration von Vorlagen und Dokumenten notwendig sind, über einen längeren Zeitraum einen «Return on Investment».

Insgesamt zeigt die Analyse, dass bei den fünf Pilotprojekten ein wirtschaftlich sinnvoller Betrieb durch einen Umstieg auf OSS-Produkte heute nicht möglich ist. Es gibt dafür zwei Gründe. Einerseits die fehlenden Eigenschaften der Alternativen, andererseits die enge, gegenseitige Kopplung der Komponenten, die – analog eines Uhrwerks – kompatibel und aufeinander abgestimmt sein müssen. Eine ICT-Infrastruktur wie jene der Stadtverwaltung besteht aus Tausenden von Komponenten, die ineinandergreifen und korrespondieren müssen. Vor diesem Hintergrund kommt der Gemeinderat gestützt auf den Projektbericht zum Schluss, dass eine vollständige Substitution von bestehenden Produkten durch OSS mit Blick auf die Anforderungen der städtischen ID in Bezug auf Funktionalität, Stabilität und Wirtschaftlichkeit zum heutigen Zeitpunkt weder sinnvoll noch zweckmässig ist. Der Gemeinderat will aber mit drei Stossrichtungen Grundlagen schaffen, um in Zukunft verstärkt auf

[1] Als Groupware bzw. Gruppen-Software (auch kollaborative Software) bezeichnet man eine Software zur Unterstützung der Zusammenarbeit in einer Gruppe über zeitliche und/oder räumliche Distanz hinweg.

Open Source-Lösungen zu setzen. Dies auch unter der Annahme, dass sich die Marktsituation weiterhin ändert und in Zukunft vermehrt kompatible OSS-Produkte verfügbar sein werden.

2. Worum es geht

Mit der Genehmigung des Investitions- und Verpflichtungskredits zum Projekt CLIMB (Client Migration Bern; Erneuerung der Bürokommunikationsplattform der Stadtverwaltung) erteilte der Stadtrat mit SRB 2015-494, Ziffer 4 vom 12. November 2015 dem Gemeinderat den Auftrag, ihm bis Ende 2017 eine detaillierte Ablösungsstrategie von Microsoft- und CITRIX-Produkten zu unterbreiten. Zudem sollte die bevorstehende Client-Migration (Projektkurzbezeichnung: CLIMB) auf diese Strategie abgestimmt werden, um bestehende Abhängigkeiten zu reduzieren. Die Ablösungsstrategie sollte mittels Pilotprojekten, Prüfung von Alternativen, Entkoppelung von Fachanwendungen, technologischen Anpassungen und Weiterbildungen erarbeitet werden. Für die Erstellung der Ablösungsstrategie sollte der Gemeinderat bis Ende Februar 2016 beim Stadtrat einen angemessenen Projektierungskredit beantragen.

Auf Antrag des Gemeinderats passte der Stadtrat mit SRB 2016-3870 vom 18. August 2016 den obigen Auftrag an, indem er eine Potenzialanalyse in Bezug auf Open Source Software (OSS) in den Fokus stellte. Durch eine praxisbezogene Potenzialanalyse und das Schaffen einer umfassenden Grundlage für zukünftige Entscheide sollte aufgezeigt werden können, welche Funktionalitäten von proprietären Produkten mittel- bis langfristig durch Open Source-Produkte ersetzt werden und damit auch, wo bzw. wie die Abhängigkeiten von marktdominanten Herstellerinnen und Herstellern gelöst werden können. Mit dem Entscheid für die Erarbeitung einer Potenzialanalyse Open Source Software bewilligte der Stadtrat einen Nachkredit zum Globalbudget 2016 der ID von Fr. 212 000.00 und nahm Kenntnis von der beabsichtigten Budgetierung von Fr. 458 000.00 für das Projekt im Globalbudget 2017 sowie vom internen Aufwand der ID von Fr. 173 000.00.

Mit diesem Auftrag startete das Projekt Potenzialanalyse Open Source Software (Projektkurzbezeichnung: POTOSS). In der Folge analysierten die ID zusammen mit der im Rahmen einer offenen Ausschreibung gewählten Firma Adfinis SyGroup AG anhand von fünf Pilotprojekten das Potenzial des Einsatzes von OSS in der Stadtverwaltung. Die Erkenntnisse sind im Expertenbericht «POTOSS. Potenzialanalyse OSS vom 23. April 2019» dargelegt. Darauf basiert der vorliegende Schlussbericht. Er beschreibt den Verlauf und die Ergebnisse der Pilotprojekte, fasst diese zusammen und macht anhand von drei Stossrichtungen Empfehlungen hinsichtlich der zukünftigen Nutzung von OSS in der Stadtverwaltung.

3. Ausgangslage

3.1. Auftrag der städtischen ID

Die ID stellen stadtweit und dienststellenspezifisch zuverlässige und moderne Kommunikations- und Informationsmittel bereit und unterhalten diese. Sie betreiben Informatik-Arbeitsplätze und -Applikationen für die Mitarbeitenden der Stadtverwaltung und der Volksschulen der Stadt Bern. In Erfüllung dieses Auftrags stehen bei jeder Implementierung einer Informatiklösung drei übergeordnete Ziele im Fokus:

1. Bereitstellen aller Funktionalitäten, welche für die Geschäftsabwicklung durch die Benutzenden erforderlich sind (Funktionalität);
2. Sicherstellen eines stabilen und reibungslosen IT Betriebs (Stabilität);
3. Anbieten der IT-Infrastruktur und Dienstleistungen mit dem besten Kosten-/Nutzenverhältnis (Wirtschaftlichkeit).

3.2. OSS in der Stadtverwaltung

In der Informatik der Stadtverwaltung werden seit Jahren sowohl Open Source-Produkte als auch proprietäre Software-Produkte eingesetzt; sie ist in diesem Sinne ein klassischer Mischbetrieb. OSS-Produkte werden insbesondere bei den Hintergrundsystemen, auf welchen Linux als Betriebssystem weit verbreitet ist oder das Datenbankmanagementsystem MariaDB genutzt wird, erfolgreich eingesetzt. Auch im Bereich der stadtweiten Applikationen nimmt OSS einen festen Platz ein. So basieren unter anderem der Internet-Auftritt oder das Intranet wie auch die interne Cloud-Lösung BernBox auf OSS. Schliesslich wurden auch einzelne Fachanwendungen OSS-basiert entwickelt und auf der Internet-Plattform GitHub publiziert (z.B. Ki-Tax).

Im Unterschied zu OSS-Produkten ist bei den herstellerspezifischen Software-Produkten der Source-Code nicht offen verfügbar, was bedeutet, dass nur die Herstellerfirmen die Software verändern können. Diese Produkte werden in der Regel durch eine Lizenz beschafft; danach fallen jährlich wiederkehrende Software-Pflegegebühren an. Damit erbringen die Firmen eine Gegenleistung in Form von Fehlerbehebungen und Weiterentwicklungen. Die jährlichen Kosten für die Lizenzgebühren belaufen sich gesamthaft auf rund 14 % des Budgets der ID.

3.3. Ausschreibung POTOSS

Abgesehen von den Fachapplikationen, welche sehr spezialisiert auf die Bedürfnisse von bestimmten Arbeitsabläufen zugeschnitten sind, setzen die ID, basierend auf den strategischen Zielen punkto Funktionalität, Stabilität und Wirtschaftlichkeit, grundsätzlich auf bewährte und verbreitete Lösungen wie z.B. die Office Suite von Microsoft oder die Virtualisierungsplattform von Citrix. Dementsprechend verfügen die Mitarbeitenden der ID über ein profundes Wissen zu diesen Software-Lösungen.

Um eine objektive Sicht zum Angebot an OSS-Lösungen zu erhalten und um auf konkrete Betriebserfahrungen zugreifen zu können, führten die ID eine offene Ausschreibung für das Projekt POTOSS durch. Im Zentrum der Ausschreibung stand die Realisierung von fünf Pilotprojekten und die technische Beratung zu OSS-Applikationen. Die Projektpartnerin oder der Projektpartner sollte zudem über grosse Erfahrung im Projektmanagement verfügen und auch Kenntnisse über die eingesetzten Applikationen der Stadtverwaltung mitbringen.

In der Schweiz gibt es eine überschaubare Anzahl potenzieller Anbieterfirmen für die Realisierung der fünf Pilotprojekte. Auf die Ausschreibung ging das Angebot der Firma Adfinis SyGroup AG ein; die Firma erhielt entsprechend den Zuschlag. Zusätzlich dazu wurde die Firma Urs Amstutz ICT AG für die externe Unterstützung beauftragt.

3.4. Grundlagen für die Erhebung der Analyse

Als professionelle Betreiberin einer komplexen Informatik-Infrastruktur verfügen die ID über Systeme, welche die Basis der Inventarinformationen des Projekts POTOSS lieferten. Dazu gehören Bestandesinformationen über die Anwenderinnen und Anwender, Inventarinformationen über die eingesetzte Hardware sowie Inventarinformationen über die zugewiesene Software.

Eine weitere Grundlage für das Projekt POTOSS bildeten die Richtlinien und Vorgaben für den Informatik-Betrieb, insbesondere auch hinsichtlich Betriebssicherheit (ICT-Security). Basierend darauf wurde ein Security Audit mit dem OSS-Client durchgeführt.

Über das Thema OSS wurde verschiedentlich geforscht und publiziert. Die Veröffentlichungen bildeten ebenfalls eine Grundlage für den vorliegenden Analysebericht. Wenn beispielsweise aus vertrauenswürdigen Quellen ersichtlich wurde, dass für die eine oder andere Lösung eine OSS-Variante technisch nicht funktionsfähig ist, wurde auf entsprechende Tests in den Pilotprojekten verzichtet.

Wichtig war des Weiteren das Wissen und die Erfahrung der Fachleute von Adfinis SyGroup AG aus vergleichbaren Kundensituationen. Dabei konnte auf praktische Erfahrung mit namhaften, teilweise auch grossen Firmen und Organisationen zurückgegriffen werden.

4. Projektziele und Vorgehen

4.1. Pilotprojekte

Im Rahmen der Ausschreibung arbeiteten die ID die einzelnen Pilotprojekte und deren Zielsetzungen detailliert aus. Bei jedem Piloten bestand der Anspruch, dass die konkrete Situation der ID betrachtet wird, dass die Pilotprojekte integriert in die Infrastruktur der ID durchgeführt werden und dass die Betriebsaspekte mitberücksichtigt werden. Folgende Pilotprojekte wurden durchgeführt:

1) Pilotprojekt A – Basis Client: Entwicklung eines OSS-Clients im Umfang des bestehenden Windows-Clients mit den Software-Produkten der Kategorie 1 (Software, die standardmässig auf allen Geräten installiert werden) und solchen der Kategorie 2 (Software, welche bei Bedarf auf die Geräte installiert werden). Dabei sollen die proprietären Software-Produkte, wo sinnvoll und machbar, durch Open Source-Produkte ersetzt werden.

2) Pilotprojekt B – Fachapplikationen: Installieren und Testen der Fachanwendungen aus der Software-Kategorie 3 (Software, welche für bestimmte Geschäftsbereiche verwendet wird, z.B. Einwohnerdienste, Grünflächenmanagement, etc.) auf dem entwickelten OSS-Client gemäss Pilotprojekt A.

3) Pilotprojekt C – Groupware: Aufbau einer OSS-Plattform für die Services Mail, Kalender, Ressourcen-, Aufgaben- und Notizenverwaltung, als Alternative zu Microsoft Outlook und Exchange.

4) Pilotprojekt D – Virtualisierung: Aufbau einer OSS-Plattform für die Applikations- und Client-Virtualisierung als Alternative zur bestehenden Citrix-Plattform und Einbindung von bereits virtualisierten Produkten der Software-Kategorien 1, 2 und 3.

5) Pilotprojekt E – CMI Axioma: Serverseitige Implementierung der proprietären Fachanwendung CMI Axioma (Geschäftsverwaltung) auf einer OSS-Plattform.

4.2. Rahmenbedingungen

Bei der Umsetzung der Pilotprojekte wurden folgende Rahmenbedingungen berücksichtig:

Prüfung von alternativen Software-Produkten

Die Prüfung von alternativen Softwareprodukten mit vergleichbarer Funktionalität wie die bisher eingesetzten proprietären Fachanwendungen wurde für alle Pilotprojekte, mit Ausnahme von Pilotprojekt E, durchgeführt, insbesondere für die Applikationen mit verbreiteter Anwendung, wie z.B. im Pilotprojekt A (Basis Client), aber auch im Pilotprojekt B (Fachanwendungen).

Entkoppelung von Fachanwendungen

Die Fachanwendungen wurden bereits bei der letzten Client Migration im Rahmen des Projekts CLIMB auf applikatorischer Ebene durch weitestgehende Applikations-Virtualisierung vom proprietären Betriebssystem des Clients entkoppelt. Es galt zu prüfen, wie gut diese Applikationen auch auf einem OSS-Client funktionieren.

Technologische Anpassungen
Der Auftrag einer Potenzialanalyse umfasst im eigentlichen Wortsinn die Untersuchung, inwieweit es möglich ist, die bestehende Software durch OSS abzulösen. Im Rahmen der Pilotprojekte wurden alle technologischen Anpassungen und Erweiterungen an der bestehenden Infrastruktur vorgenommen, die notwendig waren, um die in der Potenzialanalyse geforderten Erkenntnisse zu gewinnen.

Aus- und Weiterbildungen
Gemäss Auftrag wurde ein Teil des Budgets dafür vorgesehen, Ausbildungen durchzuführen, damit die Spezialistinnen und Spezialisten der ID zu den Pilotprojekten beitragen konnten. In der Praxis zeigte sich jedoch, dass keine Ausbildung im eigentlichen Sinn erforderlich war, sondern im «Learning by doing» bei der Umsetzung der Pilotprojekte der effektivste Weg der Wissensvermittlung lag.

Abgrenzungen und Erweiterungen
Eine wichtige Voraussetzung bei der Umsetzung der Pilotprojekte bestand darin, dass die bestehende ICT-Infrastruktur durch die vorgesehenen Pilotprojekte nicht tangiert werden durfte; der Betrieb der ICT-Systemlandschaft musste jederzeit sichergestellt werden. Zudem orientierten sich die Pilotprojekte funktional an einzelnen bestehenden Anwendungen, sie ersetzten diese jedoch im Rahmen der Potenzialanalyse nicht.

Da es das Ziel war, die bestehenden Applikationen mit der möglichst grössten Wirkung zu prüfen, wurden die Fachapplikationen, welche von weniger als fünf Personen eingesetzt werden, nicht weiter untersucht. Untersucht wurde das Potenzial für den Einsatz von OSS durch Pilotprojekte im realen Betriebsumfeld, um realitätsnähere Erkenntnisse zu gewinnen, und nicht in einer Laborumgebung, wie dies ursprünglich vorgesehen war.

Das Pilotprojekt C (Groupware Lösungen) sah ursprünglich keine Integration von Smartphones und Tablets in die Groupware Lösung vor. Da diese aber ein ausschlaggebendes Entscheidkriterium für eine OSS-Alternative sind, wurde das Pilotprojekt C um die bestehende MDM-Betriebslösung (Mobile Device Management) erweitert.

Finanzielle Auswirkungen
Die potenziellen Kostenvorteile schliesslich werden als Schätzung dargestellt. Eine genauere Berechnung hätte eine Scheingenauigkeit erzeugt, die nicht sinnvoll gewesen wäre.

4.3. Projektorganisation
Die Potenzialanalyse wurde federführend durch die externen Firmen Urs Amstutz ICT AG und Adfinis SyGroup AG in Zusammenarbeit mit Fachleuten der ID und den Applikationsverantwortlichen der Fachabteilungen erstellt. Die Fachleute der ID waren beim Aufbau der Infrastruktur massgeblich beteiligt. Die Mitarbeitenden der Fachabteilungen wurden eingeladen, um die Fachanwendungen unter dem OSS-Client zu testen und zu beurteilen, ob diese den betrieblichen Anforderungen genügen.

4.4. Projektzeitplan
Der ursprüngliche Zeitplan hatte vorgesehen, die Pilotprojekte bis Ende März 2018 abzuschliessen. Zum selben Zeitpunkt hätte auch der Abschlussbericht vorliegen sollen. Dieser Endtermin konnte wegen Ressourcenengpässen und erhöhter Komplexität nicht eingehalten werden. Die Kommission für Finanzen, Sicherheit und Umwelt (FSU) wurde an ihrer Sitzung vom 26. Februar 2018 darüber informiert, dass sich der Termin um rund sechs Monate verschieben werde. Trotz Intensivierung der Projektarbeiten konnten diese auch bis Ende September 2018 nicht fertiggestellt werden. Die Gründe dazu wurden mit Schreiben vom 15. Oktober 2018 durch die Projektverantwortlichen an die FSU dargelegt.

Insgesamt legte das Projektteam bei der Umsetzung des Gesamtprojekts und insbesondere bei der Durchführung der fünf Pilotprojekte grossen Wert darauf, sorgfältig zu arbeiten, um eine hohe Qualität der Potenzialanalyse zu gewährleisten. Zeitdruck wäre diesen Zielen abträglich gewesen. Aufgrund der umfangreichen und komplexen Arbeiten verzögerte sich der Schlussbericht deshalb gegenüber dem ursprünglichen Zeitplan um rund ein Jahr.

4.5. Projektkosten

Für die Umsetzung der Pilotprojekte und die Erarbeitung des Abschlussberichts standen total Fr. 843 000.00 zur Verfügung. Hierfür wurde kein Projektierungskredit beantragt, sondern im Jahr 2016 das Globalbudget der ID mittels Nachkredit um Fr. 220 000.00 erhöht. Zudem wurden im Rahmen des Budgets 2017 Fr. 458 000.00 vorgesehen sowie ein ID-interner Aufwand von Fr. 173 000.00. Weil sich die Projektarbeiten verzögerten, mussten Nachkredite für die Globalbudgets 2018 und 2019 beantragt werden. Die effektiven Kosten des Gesamtprojekts werden jedoch unter den veranschlagten Totalkosten für das Projekt abgeschlossen werden können.

5. Erkenntnisse aus den Pilotprojekten

5.1. Pilotprojekt A – Basis Client

Ausgangslage

Ein OSS Client ist nur dann ein vollwertiger Ersatz des bestehenden Windows-Clients, wenn die Bedürfnisse der Anwendenden abgedeckt werden und die informatikgestützten Arbeiten mit gleicher Produktivität wie auf dem proprietären Client erfolgen können. In einem Benutzungskonzept ist festzuhalten, welche Personen auf welche Applikationen und Daten zugreifen dürfen (Authentisierung und Autorisierung). Betrieblich ist sicherzustellen, dass die Clients einwandfrei funktionieren. Ein Rollout von neuen Geräten muss automatisiert und einfach erfolgen können. Die Clients und Applikationen sind regelmässigen Aktualisierungen unterworfen. Die Stadt betreibt über 2 200 Clients in einem Active Directory von Microsoft, ein neuer Client muss sich darin integrieren lassen. Letztlich sind die Clients so sicher aufzusetzen, dass damit verarbeitete Daten nicht in falsche Hände geraten (Verschlüsselung).

Das Applikationsinventar der Stadt umfasst total etwa 230 Applikationen. Es gibt 30 Applikationen der Kategorie 1 und 17 Applikationen der Kategorie 2 (siehe Kapitel 41). Im Rahmen von Pilot A muss ein Client die Funktionalitäten der Kategorie 1 sowie der Kategorie 2 abdecken. Software der Kategorie 1 wird auf jedem Client installiert, während jene der Kategorie 2 auf den meisten Clients installiert wird.

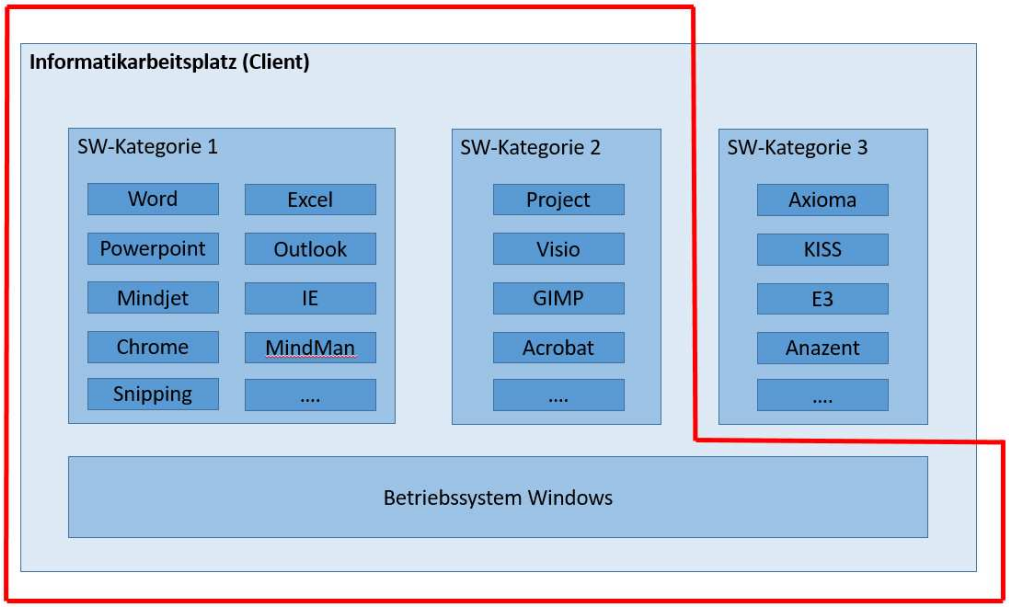
Im Rahmen des Projekts CLIMB wurden ca. 2/3 der festen Arbeitsplätze auf Thin-Clients[2] umgestellt. Die Linux-basierten Geräte verfügen damit bereits heute über ein OSS-Betriebssystem. Aus verschiedenen Gründen (Mobilität, Leistung, spezielle Hardware) sind nach wie vor ca. 800 Fat-Clients[3] im Einsatz (Desktops oder Notebooks).

[2] Ein Thin Client ist ein Arbeitsplatz-Computer ohne lokale Software-Installationen, das auf die Hilfe eines Servers angewiesen ist, um seine Aufgaben zu erfüllen.

[3] Ein Fat-Client ist ein Arbeitsplatz-Computer (Desktop oder Notebook) mit lokaler Speicherung der Software und Rechnerleistung.

Pilotbeschrieb

Im Pilotprojekt A wurden die folgenden Komponenten geprüft:



IE: Internet Explorer (Browser von Microsoft) / MinMan: Software zur Erstellung von Mindmaps / GIMP: Bildbearbeitungssoftware / KISS: Klienten-Informationssystem im Sozialwesen / E3: Zeit- und Leistungserfassungssoftware

Als erstes wurde ein OSS-Client mit den wichtigsten Eigenschaften eines professionellen Arbeitsplatzes weitgehend automatisiert von der «leeren» Hardware aufgebaut. Er verfügte über die notwendigen Funktionalitäten wie Globale Einstellungen, Single Sign on[4], Internet Browser und Citrix-Receiver. Aufgrund der Anforderung, wonach ein OSS-Client so sicher sein muss wie der aktuelle Windows-Client, wurde dieser nach der Installation einem externen Sicherheits-Auditing unterzogen.

Als OSS-Betriebssystem für den Client wurde openSUSE gewählt, weil zum Zeitpunkt des Entscheids SUSE die einzige Linux-Plattform war, auf der in Zukunft SAP-Datenbanken betrieben werden können und es sinnvoll ist, die Anzahl verschiedener Distributionen in einer Organisation möglichst tief zu halten.

Schliesslich wurde im Rahmen des Pilotprojekts A das im OSS-Umfeld weit verbreitete LibreOffice eingehend getestet.

Testergebnisse

Der Basis-Client bietet 30 Applikationen der Kategorie 1 als Grundausstattung. Es handelt sich dabei um verbreitete Funktionalitäten, weshalb 20 OSS-Alternativen gefunden werden konnten. Eingehende Tests zeigten jedoch auf, dass viele dieser OSS-Alternativen Einschränkungen aufweisen und für den professionellen Einsatz nicht genügen (Kompatibilitätsprobleme zu bestehenden Dokumenten, einschneidende funktionale Mängel, fehlerhafte Datenverarbeitung). Acht OSS-Alternativen könnten mit gewissen Einschränkungen für den städtischen Betrieb eingesetzt werden.

Die 17 Applikationen der Kategorie 2 bieten Grundfunktionalitäten an wie z.B. Visio oder MS Project. Hier wurden drei native (die gleiche Software auf Linux installierbar) und sieben OSS-Alternativen getestet. Von letzteren hat sich lediglich eine Applikation als geeignet erwiesen.

LibreOffice als OSS-Alternative zu Microsoft Office genügt den Bedürfnissen der Anwendenden zu einem grossen Teil in einem isolierten Bereich. Ist ein Datenaustausch mit externen Stellen erforderlich, oder müssen Daten von Fachapplikationen exportiert oder importiert werden, ist dies jedoch nur

[4] «Einmalanmeldung» bedeutet, dass eine Benutzerin nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die sie berechtigt ist zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen.

sehr erschwert möglich, weil z.B. bei wechselseitiger Bearbeitung und damit wiederholter Konversion der Datenformate Formatierungsmängel entstehen, welche wiederholt manuell korrigiert werden müssen.

Im Rahmen des Sicherheits-Audits wurde festgestellt, dass der OSS-Client grundsätzlich so aufgesetzt werden kann, dass er die Sicherheitsvorgaben erfüllt. Sicherheitsfunktionen umfassen unter anderem Screenlock (Bildschirmsperre), Disk Encryption (Festplattenverschlüsselung), Firewall (Zugangsschutzsystem), Antivirus Software und die Möglichkeit, regelmässig Security Patches und Updates (Sicherheitsanpassungen) einzuspielen.

Chancen
Der Einsatz von OSS anstelle von proprietärer Software bietet im Pilotprojekt A die Chance, sich schritt- bzw. teilweise aus der Abhängigkeit von marktdominanten Herstellerinnen und Herstellern (in erster Linie Microsoft) zu lösen. Darüber hinaus ist die Benutzendenoberfläche von LibreOffice im Vergleich zu MS Office intuitiver. Weitere Vorteile sind der potenziell stärkere Kundenfokus bei kleineren OSS-Support-Anbietenden sowie der Wegfall der Formatumwandlung bei der Langzeitarchivierung.

Risiken
Der Einsatz von OSS birgt im Pilotprojekt A jedoch auch Nachteile und Risiken. So ist der Dokumentenaustausch mit anderen Abteilungen oder externen Stellen aufgrund des nicht identischen Datenformats nicht durchgängig. Dies würde zu Mehraufwand, Produktivitätsverlust und Unzufriedenheit bei den Benutzenden führen. Darüber hinaus müssten die Schnittstellen zu Fachapplikationen mit entsprechendem Aufwand angepasst werden; zudem wäre dies nicht für jede Fachapplikation möglich. Schliesslich ist das Schaffen von neuen Abhängigkeiten von kleineren, auf OSS-Produkte spezialisierten Unternehmen sowie der Parallelbetrieb von zwei Client-Plattformen zu erwähnen. Letzteres ist technisch komplexer und damit fehleranfälliger sowie teurer.

Finanzen
Ausgehend von der Annahme, dass rund 500 Clients von Microsoft auf OSS umgestellt würden, könnte mit einer Einsparung von wiederkehrenden Microsoft Windows- und Office-Lizenzen von ca. Fr. 70 000.00 gerechnet werden. Auf der Aufwandseite ist mit erhöhten Investitionen für den Plattformaufbau von rund Fr. 687 000.00, wiederkehrenden Zusatzkosten durch den Betrieb zusätzlicher Plattformen von rund Fr. 343 000.00 sowie Investitionen für den Wissensaufbau von ca. Fr. 1 164 000.00 zu rechnen.

Empfehlung aus dem Expertenbericht
Der Expertenbericht empfiehlt den Wechsel auf den OSS Basis Client nicht, da er als primärer bzw. einziger Arbeitsplatz nur für wenige Mitarbeitende brauchbar sei. Die steigenden Kosten würden den Mehrwert nicht rechtfertigen. Als Alternative zu Windows könne LibreOffice jedoch angeboten werden.

Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Der Dokumentenaustausch mit internen und externen Stellen ist nicht durchgängig.
Sicherstellen des stabilen Informatikbetriebs	Die Stabilität kann mit dem Aufbau von Know how sichergestellt werden. Die Komplexität des Betriebs nimmt zu.
Wirtschaftlichkeit	Die Investitionen in den Plattformaufbau führen zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden. Ein erster Schritt wäre möglich. Gleichzeitig können neue Abhängigkeiten zu kleineren, auf OSS Produkte spezialisierten Firmen entstehen.

5.2. Pilotprojekt B – Fachapplikationen

Ausgangslage

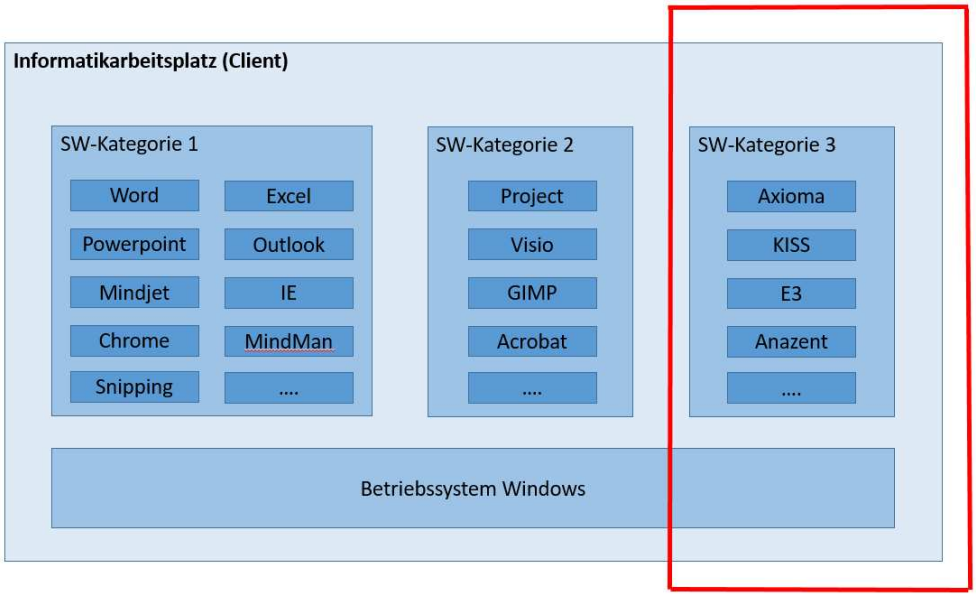
Die Stadtverwaltung umfasst eine Vielzahl von Aufgaben, die von den einzelnen Dienststellen wahrgenommen werden. Deren Mitarbeitende sind auf Fachapplikationen angewiesen, mit welchen sie ihre täglichen, spezialisierten Aufgaben abwickeln. Die Fachapplikationen werden von den Dienststellen in Bezug auf ihre speziellen Bedürfnisse definiert und beschafft. Die ID stellen die Applikationen auf den Clients der Mitarbeitenden zur Verfügung; für die Geschäftsabwicklung der ganzen Dienststelle sind sie jedoch zwingend notwendig.

Aktuell beläuft sich das Inventar der Fachapplikationen auf rund 180. Die Hälfte dieser Fachapplikationen sind als virtualisierte Applikationen verfügbar. Um diese mit einem OSS-Client zu nutzen, bietet Citrix den entsprechenden OSS-Client an. Ein Fünftel der Fachapplikationen sind Webapplikationen. Auch diese lassen sich auf einem OSS-Client und dem entsprechenden Browser nutzen.

Für die proprietären Fachapplikationen der Stadt gibt es heute keine nativen OSS-Lösungen (die gleiche Software auf Linux installierbar) und auch nur sehr vereinzelt echte OSS-Alternativen (z.B. Ki-Tax).

Pilotbeschrieb

Pilotprojekt B fokussierte auf die folgenden Komponenten:



IE: Internet Explorer (Browser von Microsoft) / MinMan: Software zur Erstellung von Mindmaps / GIMP: Bildbearbeitungssoftware / KISS: Klienten-Informationssystem im Sozialwesen / E3: Zeit- und Leistungserfassungssoftware

Der Test bestand darin, zu überprüfen, ob die Fachapplikationen auf dem OSS-Client einwandfrei funktionieren. Bei den Fachapplikationen, welche nur lokal installiert werden können, wurde geprüft, ob sie sich mit Hilfe einer Übersetzungssoftware (Crossover) auf einem OSS-Client funktionsfähig sind. Die Applikationsverantwortlichen der Dienststellen definierten die notwendigen Tests und führten sie mit Unterstützung eines Spezialisten von Adfinis SyGroup AG durch.

Testergebnisse
Im Rahmen der Tests wurden die Applikationen, welche von fünf oder mehr Anwenderinnen und Anwendern eingesetzt wurden, überprüft. Davon war die Hälfte, teilweise mit Einschränkungen, funktionsfähig und nutzbar. Die andere Hälfte war für den praktischen Einsatz nicht funktionsfähig oder nicht testbar.

Chancen
Da viele Fachapplikationen im Rahmen des Projekts CLIMB virtualisiert wurden, können diese gemäss den Tests im «Citrix-Fenster» auch auf einem OSS-Basis-Client benutzt werden. Sie stellen somit kein Hindernis für die Einführung eines OSS-Basis-Clients (gemäss Pilotprojekt A) dar. Bei neu zu beschaffenden Fachapplikationen kann die Kompatibilität zum OSS-Client gefordert werden. Im Fall einer Neuentwicklung als OSS-Applikation könnten diese zusammen mit den Dienststellen anderer öffentlicher Verwaltungen entwickelt und im Internet publiziert werden.

Risiken
Der Nachteil der Nutzung von Fachapplikationen auf einem Linux-Client besteht darin, dass Web-Applikationen, die nur für einen bestimmten Browser unter Windows entwickelt wurden, nicht korrekt dargestellt werden oder nicht funktionieren. Auch gewisse Citrix-Fachapplikationen funktionieren nicht oder nicht einwandfrei.

Fachapplikationen, welche lediglich als Windows Versionen verfügbar sind, konnten in den wenigsten Fällen mit Hilfe einer Übersetzungssoftware (Crossover) auf dem Linux Client funktionsfähig installiert werden. Sie können mit einem OSS-Client nicht genutzt werden. Insgesamt wird Crossover von den Applikationsherstellenden nicht unterstützt und verunmöglicht damit einen professionellen Einsatz.

Finanzen
Die Fachapplikationen werden von den Dienststellen beschafft und lizenziert. Ein Einsparpotenzial von Lizenzen in diesem Bereich besteht nicht. Hingegen müssen kleine Investitionen für die Anpassung der Plattformen (Citrix, WEB) getätigt werden, damit die webbasierten oder auf Citrix virtualisierten Fachapplikationen auf einem OSS-Client genutzt werden können.

Empfehlung aus dem Expertenbericht
Der Expertenbericht kommt bei der Auswertung von Pilotprojekt B zum Schluss, dass OSS-Clients ausschliesslich für diejenigen Mitarbeitenden eingesetzt werden könnten, deren Fachapplikationen auf einem Browser oder unter Citrix einwandfrei funktionieren, was jedoch aufgrund der Empfehlung aus Pilotprojekt A «ein theoretisches Gedankenspiel» sei. Die Experten empfehlen aus diesem Grund, dass OSS-Browser daher bereits bei den Beschaffungen Beachtung finden sollen, wobei der Support von Web-Applikationen durch den Hersteller sicherzustellen sei.

Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Die Fachapplikationen können teilweise auf einem OSS-Client benutzt werden. Heute gibt es kaum OSS-Alternativen.
Sicherstellen des stabilen Informatikbetriebs	Die Stabilität des IT Betriebs wird nicht verändert.
Wirtschaftlichkeit	Es sind Investitionen erforderlich. Sie führen jedoch zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden.

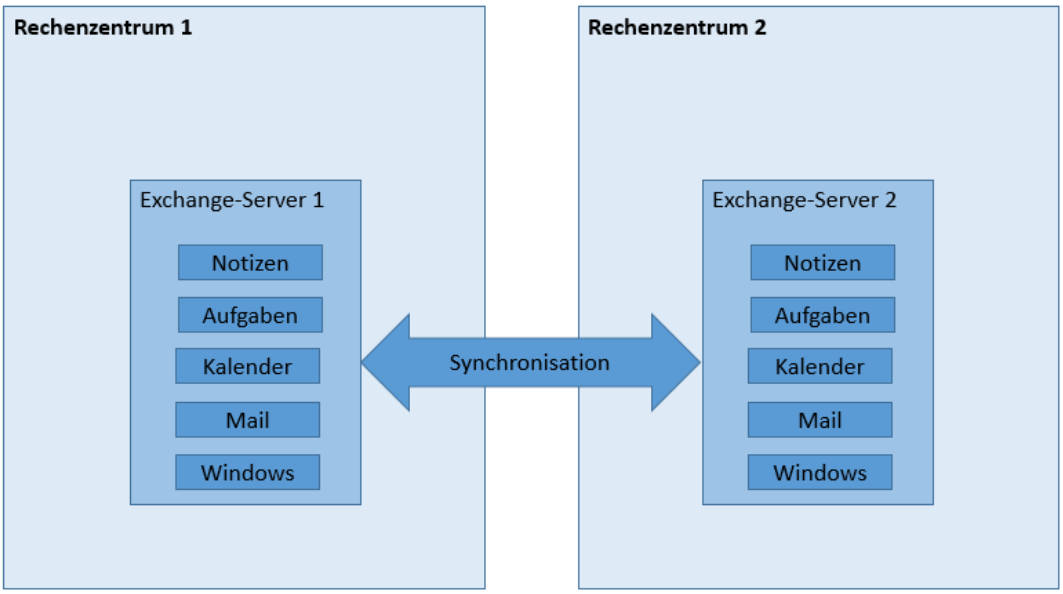
5.3. Pilotprojekt C – Groupware

Ausgangslage

Die Kernfunktionen einer Groupware sind E-Mail (mit Adressbüchern) und Kalender. Weitere Funktionen sind Aufgaben und Notizen. Deren Benutzung ist aber je nach Person sehr unterschiedlich. Die ID betreiben aktuell eine von Microsoft angebotene Exchange-Infrastruktur in den eigenen Rechenzentren mit Outlook als Client-Software. Die wichtigste Anforderung aus Betreibersicht ist die Verfügbarkeit: der Betrieb kann ohne Groupware nicht gewährleistet werden.

Pilotbeschrieb

Im Rahmen des Pilotprojekts C wurde ein redundanter Aufbau des Groupware-Systems in den zwei städtischen Rechenzentren vorgenommen. Dabei wurden folgende Komponenten geprüft:



Es gibt aktuell mehrere OSS-Produkte, welche als Ersatz für Microsoft Exchange in Frage kommen. Da zu Projektbeginn kein detaillierter Anforderungskatalog vorlag, hat Adfinis SyGroup AG aufgrund der eigenen Erfahrungen das Produkt Open Xchange für die Demo-Installation bei der Stadt ausgewählt. Einerseits ist dieses Produkt bei Internet-Providern im grossen Stil im Einsatz, was bedeutet, dass es eine grosse Basis an bestehenden Installationen gibt. Andererseits hat eine vergleichende Anforderungsanalyse Ende 2016 bei einem Kunden mit ca. 30 000 Postfächern Open Xchange als bestes OSS-Produkt ergeben. Obwohl die Anforderungen dieses Kunden mit denjenigen der Stadt nicht deckungsgleich sind, war das doch einer der Gründe für die Wahl von Open Xchange. Beim erwähnten Kunden ist dieses System über ein Jahr erfolgreich im Einsatz.

Testergebnisse
Der Pilot C hat gezeigt, dass eine OSS-Groupware-Lösung aufgebaut und mit der notwendigen Redundanz betrieben werden kann. Die meisten benötigten Funktionen sind implementiert. Als betriebsverhindernde Einschränkung wird die Tatsache gewertet, dass unter anderem wichtige Funktionen wie z.B. Send on behalf (im Auftrag versenden) nicht verfügbar sind.

Chancen
Der Einsatz von OSS anstelle von proprietärer Software bietet im Pilotprojekt C die Chance, die Abhängigkeit von marktdominanten Herstellerinnen und Herstellern zu verkleinern und die neu entstehende Wettbewerbssituation zu nutzen.

Risiken
Der Einsatz von OSS ist mit dem Nachteil verbunden, dass Open Xchange nicht alle Funktionalitäten von Microsoft Exchange anbietet. Die Integration von Mobilgeräten, Sitzungszimmern und Call Centern funktioniert zwar, der Support durch die Herstellerinnen und Hersteller ist jedoch nicht gewährleistet. Dies ist insofern von grosser Bedeutung, weil die mobile Nutzung künftig zu- und nicht abnehmen wird.

Finanzen
Eine Umstellung würde zu einer jährlich wiederkehrenden Einsparung der Microsoft Windows Lizenzen von ca. Fr. 4 000.00 führen. Demgegenüber stehen jährliche Subscriptions-Kosten von rund Fr. 160 000.00 an. Einmalig würden Investitionskosten für den OSS-Plattformaufbau ca. Fr. 621 000.00 sowie für den Wissensaufbau über Open Xchange von ca. Fr. 898 000.00 anfallen.

Empfehlung aus dem Expertenbericht
Die Experten kommen zum Schluss, dass OpenXchange punkto Kern-Funktionalität und Stabilität eine durchaus gangbare Variante wäre. Dennoch raten sie zum heutigen Zeitpunkt von einem Wechsel ab. Einerseits ist der Support für die integrierten Umsysteme (Mobilgeräte, Call-Center, Serienbriefe etc.) nicht gewährleistet. Zudem wirft der Expertenbericht die Frage auf, ob die Anwendenden die fehlenden Funktionalitäten (z.B. Send on behalf) akzeptieren würden. Sollte OpenXchange eingeführt werden, müsse es daher in ein Vorprojekt eingebettet sein.

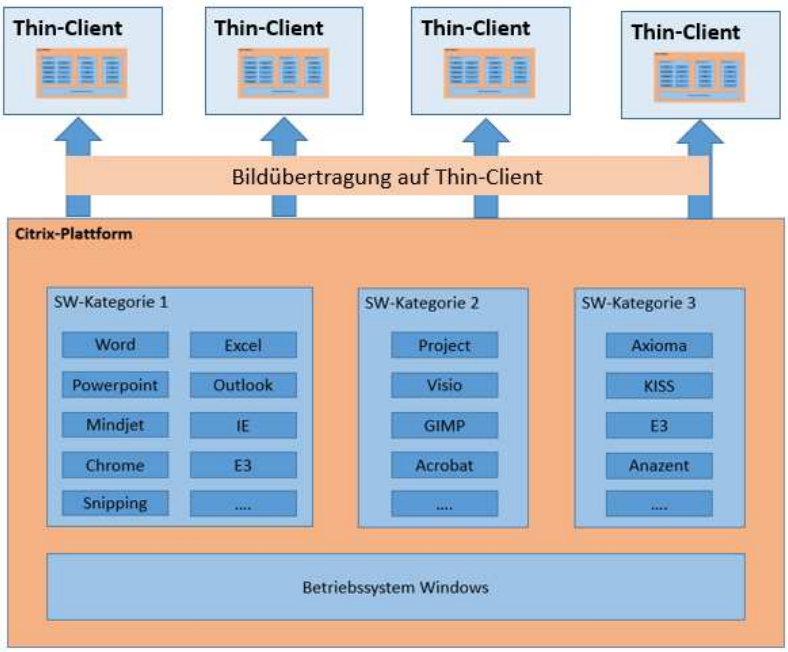
Übersicht

Kriterium	**Begründung**
Funktionalität für die Geschäftsabwicklung	Es fehlen wichtige Funktionen (z.B. «im Auftrag versenden») und Desktop-Integrationen.
Sicherstellen des stabilen Informatikbetriebs	Die Kernfunktionen sind verfügbar, aber es gibt keinen Support für serverseitige Integrationen.
Wirtschaftlichkeit	Eine Migration ist aufwändig, die Kosten für den Betrieb sind vergleichbar.
Abhängigkeit von dominanten Marktteilnehmenden	Sämtliche Daten werden in offenen Formaten gespeichert und sind über offene Schnittstellen zugreifbar.

5.4. Pilotprojekt D – Virtualisierung

Ausgangslage
Bei der Virtualisierung von Systemen geht es im Wesentlichen darum, statt einer physischen Umgebung eine simulierte oder virtuelle Informatik-Umgebung herzustellen. Es gibt verschiedene Kategorien der Virtualisierung. Mit der Desktop-Virtualisierung wird durch einen zentralisierten Server individualisierte Rechen- und Speicherkapazität für einen einzelnen Arbeitsplatz geliefert und verwaltet.

Ähnliches erfolgt bei der Server-Virtualisierung: ein einzelner physischer Server (Host) wird in mehrere virtuelle Server (Clients) aufgeteilt. Eine weitere Kategorie ist die Applikations-Virtualisierung, die einzelne Anwendungen (und nicht ganze Sessions) zum Endgerät der Anwendenden bringt.



Pilotbeschrieb

Im Fokus der Tests für den Aufbau einer OSS-Plattform als Alternative zur bestehenden Citrix-Plattform und der Einbindung von bereits virtualisierten Produkten der Software-Kategorien 1 - 3 stand zum einen die Applikations-Virtualisierung, zum anderen die Server-Virtualisierung. Als Produkt wurde die Red Hat Virtualization (RHV) gewählt. Das Produkt hat sich als zuverlässiges System etabliert. RHV kann (wie auch Citrix und VMware) sowohl Windows wie auch Linux virtualisieren.

Testergebnisse

Die OSS-Variante erfüllt die Anforderungen der Client- und Applikationsvirtualisierung nicht. Insbesondere gibt es keinerlei spezifischen Support für Windows als Client-Betriebssystem, also weder ein Profil-Management noch eine Windows-Applikationsvirtualisierung.

Chancen

Das grundsätzliche Prinzip der Applikationsvirtualisierung existiert in reinen Unix-Umgebungen (Client und Server) seit etwa 35 Jahren. Diese erfüllt aber weder die heutigen Anforderungen, noch funktioniert es für Windows-Applikationen.

Risiken

Es gibt aktuell kein OSS-Produkt, das die Windows-Applikationsvirtualisierung unterstützt.

Finanzen

Der Einsparung von wiederkehrenden Citrix-Lizenzen von ca. Fr. 140 000.00 und der wiederkehrenden Zusatzkosten durch den Betrieb zusätzlicher Plattformen von ca. Fr. 147 000.00 stehen erhöhte Investitionen für den Plattformaufbau von ca. Fr. 480 000.00 gegenüber. Die Kosten für die Subscriptions wiegen die Lizenzkosten auf, d.h. die Betriebskosten bleiben gleich.

Empfehlung aus dem Expertenbericht

Der Expertenbericht kommt zum Schluss, dass eine OSS-Lösung für die Windows-Applikationsvirtualisierung zum heutigen Zeitpunkt nicht empfohlen werden kann. Sollte dereinst nicht mehr Windows als Client-Betriebssystem virtualisiert werden müssen, werde die Auswahl

von geeigneten Virtualisierungslösungen jedoch grösser. Insofern sei die weitere Entwicklung in diesem Bereich genau zu beobachten.

Übersicht

Kriterium	**Begründung**
Funktionalität für die Geschäftsabwicklung	Die Funktionalität für eine Client Virtualisierung ist ungenügend.
Sicherstellen des stabilen Informatikbetriebs	Die Stabilität kann mit dem Aufbau von Know How sichergestellt werden. Die Komplexität des Betriebs nimmt zu.
Wirtschaftlichkeit	Die Investitionen in den Plattformaufbau führen zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden.

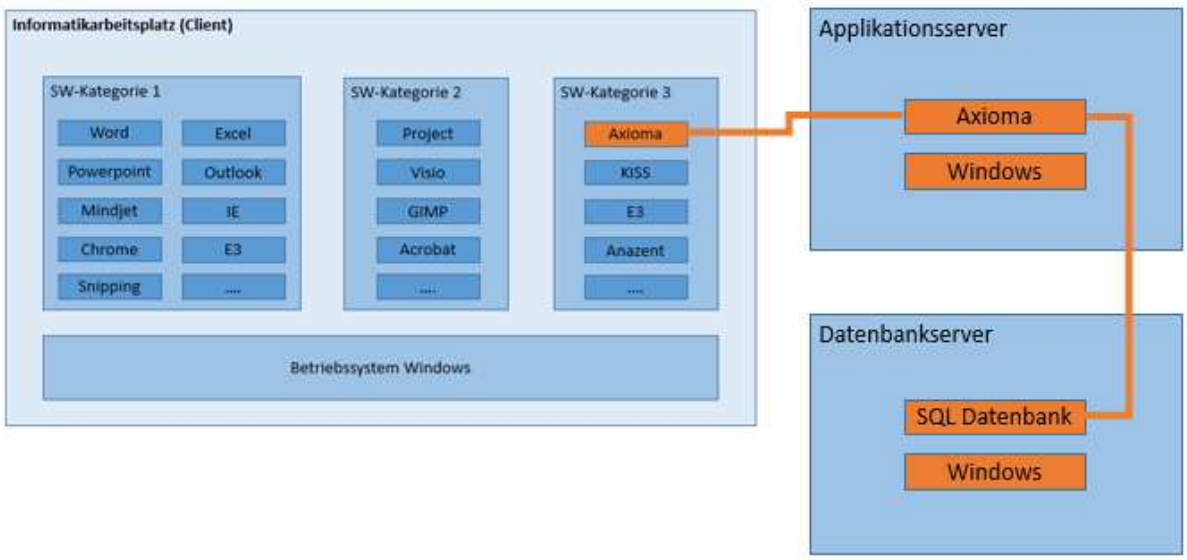
5.5. Pilotprojekt E – CMI AXIOMA

Ausgangslage

CMI Axioma wird von der Stadt Bern für die Verwaltung der politischen Geschäfte benutzt. Die aktuelle Version besteht aus einer klassischen Drei-Schicht-Architektur, bestehend aus den drei Komponenten Client, Applikationsserver und Datenbank.

Pilotbeschrieb

Im Rahmen von Pilotprojekt E wurde die proprietäre Fachanwendung CMI Axioma (Geschäftsverwaltung) auf eine OSS-Plattform implementiert. Dabei wurde nach Rücksprache mit der Herstellerfirma CM Informatik AG (CMI) der Aspekt Client-Programm nicht weiter in die Analyse einbezogen. CMI ist daran, einen HTML-5 basierten Axioma-Client zu entwickeln, welcher mit einem Browser auf einem Linux-Betriebssystem problemlos benutzt werden könnte.



In Bezug auf den Applikationsserver wäre ein Transfer auf eine Linux-Plattform sehr interessant. Dieser basiert technisch auf Microsoft .NET[5] (dot net). Leider gibt es für Linux nur die sogenannte

[5] Microsoft .NET dient als Sammelbegriff für mehrere von Microsoft herausgegebene Software-Plattformen, die der Entwicklung und Ausführung von Anwendungsprogrammen dienen, Produkte, Frameworks, Programmiersprachen, Werkzeuge und Technologien.

.NET Core-Funktionalität[6]. Diese bietet nur einen Teil der Funktionalität von .NET – was aber für Axioma nicht reicht.

Im Bereich der Datenbank wurde zunächst die Möglichkeit analysiert, auf eine OSS-Datenbank zu wechseln (zum Beispiel postgreSQL[7] oder mariaDB). Da sich alle Datenbank-Implementationen mehr oder weniger unterscheiden, wären bei einem Wechsel Anpassungen am Programmcode auf dem Applikations-Server notwendig gewesen. Dies hätte einen substantiellen Beitrag von CMI erfordert. CMI sieht aktuell aber keinen Bedarf nach einer Unterstützung von OSS-Datenbanken. Schliesslich wurde ein neues Betriebssystem des Datenbankrechners geprüft, d.h. installiert und mit dem Testsystem verbunden: die von Microsoft seit ein paar Jahren angebotene Variante MSSQL auf Linux.

Ergebnisse
Die Herstellerfirma CMI bietet für den Betrieb von Axioma keine Möglichkeit, dieses auf einem OSS-Betriebssystem lauffähig zu machen. Der Datenbankrechner liesse sich jedoch auf Linux portieren (MSSQL auf Linux von Microsoft).

Chancen
Der Einsatz von OSS anstelle von proprietärer Software bietet auch im Pilotprojekt E die Chance, sich durch den Transfer der Datenbank auf ein Linux System schrittweise aus der Abhängigkeit von marktdominanten Herstellerinnen und Herstellern zu lösen.

Risiken
Der Einsatz eines OSS-Betriebssystems birgt im Pilotprojekt E keine erkennbaren Risiken.

Finanzen
Im Bereich von CMI Axioma würden keine Einsparung von Lizenzen anfallen, hingegen müssten Investitionen in die Datenbank-Migration getätigt werden.

Empfehlung aus dem Expertenbericht
Die Migration der Datenbank auf Linux wird von den Experten nicht empfohlen, da nur eine marginale Kosteneinsparung hinsichtlich Lizenzen erzielt werden könne.

Übersicht

Kriterium	**Begründung**
Funktionalität für die Geschäftsabwicklung	Die Funktionalität ist durch die Portierung auf ein OSS Betriebssystem nicht tangiert
Sicherstellen des stabilen Informatikbetriebs	MS SQL wird für Linux angeboten. Der Support durch CMI AXIOMA ist nicht gewährleistet.
Wirtschaftlichkeit	Investition in die Datenbank-Migration. Keine Einsparung von Lizenzkosten.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden. Ein erster Schritt wäre möglich.

[6] Microsoft .NET Core ist eine freie und quelloffene Software-Plattform (innerhalb) der .NET-Plattform, die zur Entwicklung und Ausführung von Anwendungsprogrammen dient und unter der Koordination von Microsoft entwickelt wird.

[7] SQL (Structured Query Language) ist eine Datenbanksprache zur Definition von Datenstrukturen in relationalen Datenbanken sowie zum Bearbeiten (Einfügen, Verändern, Löschen) und Abfragen von darauf basierenden Datenbeständen.

6. Kostenüberlegungen

6.1. Lebenszyklen

Die rasante Entwicklung der IT bringt es mit sich, dass die Erneuerungszyklen von Software immer kürzer werden. Aktuell werden die Softwarereleases in monatlichen Abständen aktualisiert. Dahingegen hat sich die Lebensdauer von Hardware in einem Bereich von drei bis sechs Jahren eingependelt. Jedes Unternehmen ist gefordert, im Rahmen dieser Zyklen Ersatzbeschaffungen zu tätigen. Wenn es sich dabei um eine Erweiterung eines bestehenden Produkts handelt, entstehen keine Migrations- und Ausbildungskosten, sondern höchstens ein überschaubarer Testaufwand. Die Einführung eines OSS-Produkts jedoch zieht den Aufbau der Plattform sowie Migrations- und Ausbildungskosten nach sich. Diese Investitionen vor Ablauf eines Lebenszyklus zu machen, wäre aus einer Kostenperspektive dann sinnvoll, wenn sich sofort spürbare Einsparungen im Betrieb realisieren liessen, die in kurzer Zeit amortisiert wären. Dies ist aber nicht der Fall. Aus diesem Grund ist es sinnvoll, eine Umstellung auf OSS-Produkte dann vorzunehmen, wenn durch eine notwendige Ersatzbeschaffung neue Investitionen getätigt werden müssen.

6.2. Mischbetrieb

Die Untersuchungen im Rahmen dieser Studie zeigen auf, dass eine vollständige Substitution von bestehenden Produkten durch OSS nicht realisierbar ist. Um einen kostenoptimierten IT-Betrieb zu erreichen, ist die Anzahl unterschiedlicher Applikationen möglichst tief zu halten. Der durch den Einsatz von OSS-Produkten zwangsläufig erforderliche Mischbetrieb widerspricht diesem Grundsatz und führt zu suboptimalen Betriebskosten.

6.3. Investitionen

Bei der Ermittlung des Investitionsbedarfs für die Einführung von OSS-Produkten wurde versucht, die Differenz gegenüber der Einführung von den bisher eingesetzten Produkten abzuschätzen.

Während das Einsparpotenzial vor allem im Entfall von hohen Lizenzgebühren liegt, sind in diversen Bereichen zusätzliche Investitionen zu tätigen:

- Aufbau von Wissen bei den Administratorinnen und Administratoren sowie dem Supportpersonal, da diese in der Regel mit den OSS-Produkten nicht vertraut sind;
- Schaffen von ein bis zwei zusätzlichen Stellen für das Client-Engineering;
- Zusätzlicher externer Support für den initialen Aufbau der neuen Plattformen;
- Ausbildung der Anwendenden, da sie die Produkte nicht kennen;
- Migration von Daten (Vorlagen, Dokumente) auf die einzusetzenden OSS-Produkte;
- Anpassung von Schnittstellen der OSS-Produkte z.B. zu den Fachapplikationen.

Übersicht der Investitionen

In der nachfolgenden Tabelle werden die geschätzten und summierten Investitionskosten je Pilotprojekt dargelegt. Details hierzu sind dem POTOSS-Abschlussbericht zu entnehmen.

Zusätzliche Investitionen zum Aufbau von OSS-Plattformen in Franken					
Pilot	**Adminschulung**	**Enginneering/ Systemaufbau**	**Migration/ Schnittstellen**	**Benutzerschulung**	**Total**
A	90 000.00	535 000.00	152 000.00	1 074 000.00	1 851 000.00
B	0.00	110 000.00	113 000.00	0.00	223 000.00
C	123 000.00	267 000.00	354 000.00	775 000.00	1 519 000.00
D	66 000.00	414 000.00	0.00	0.00	480 000.00
E	0.00	3 000.00	1 000.00	0.00	4 000.00
Total	**279 000.00**	**1 329 000.00**	**620 000.00**	**1 849 000.00**	**4 077 000.00**

6.4. Betriebskosten

Bei der Ermittlung der Betriebskosten von OSS-Produkten wurde versucht, die Differenz gegenüber den bisher eingesetzten Produkten abzuschätzen. Das Einsparpotenzial liegt im Entfall der wiederkehrenden Lizenzkosten von proprietären Produkten sowie im Entfall von wiederkehrenden Wartungskosten. Zusätzliche Betriebskosten entstehen aufgrund des externen Supports für den Betrieb der neuen Plattformen (Subscriptions) sowie aufgrund des Betriebs und Supports von zwei Plattformen, weil die Ablösung nicht vollständig möglich ist.

Übersicht der jährlichen Betriebskosten

In der nachfolgenden Tabelle werden die geschätzten und summierten Betriebskosten je Pilotprojekt dargelegt. Details hierzu sind dem POTOSS-Abschlussbericht zu entnehmen.

Pilot	**Reduktion bisheriger Betriebsaufwand pro Jahr in Franken**			**Zusätzlicher Betriebsaufwand mit OSS pro Jahr in Franken**			**Vergleich in Franken**
	Lizenzen	**Admin/ Support**	**Total**	**Subscriptions**	**Admin/ Support**	**Total**	
A	-70’000	-	-70'000	123'000	290'000	413'000	343'000
B	-	-	-	-	-	-	-
C	-4’000	-73'000	-77'000	164'000	73'000	237'000	160'000
D	-140'000	-	-140'000	117'000	23'000	147'000	7'000
E	-	-	-	1’000	-	1’000	1’000
Total	**-214'000**	**-73'000**	**-287'000**	**405'000**	**386'000**	**798'000**	**511'000**

6.5. Indikativer Kostenvergleich

Zum heutigen Zeitpunkt kann ein indikativer Kostenvergleich als Entscheidunterstützung erstellt werden. Dieser entspricht der Zielsetzung einer Potenzialanalyse, kann jedoch nicht alle Variablen und die Preisveränderungen bis zur konkreten Umsetzung genau beziffern. So wäre bei einer konkreten Umsetzung zu beachten, dass sich die Marktsituation und die Preise verändern können. Ebenso ist zu berücksichtigen, dass die Migrationskosten (Datenmigration, Schnittstellenanpassung) nur geschätzt sind – vor dem Zeitpunkt einer allfälligen Umsetzung wären diese genauer zu ermitteln.

7. Schlussfolgerungen

7.1. Schlussfolgerungen aus den Pilotprojekten

Die Potenzialanalyse hatte zum Ziel, eine umfassende Untersuchung zum Einsatz von Open Source Software (OSS) in der Stadtverwaltung Bern durchzuführen. Dem Auftrag des Stadtrats vom 18. August 2016 entsprechend, wurde diese anhand von fünf Pilotprojekten vorgenommen. Die Erwartung bestand darin, dass es möglich sein sollte, sich bei einer nächsten Ersatzbeschaffung von den marktdominanten Herstellerfirmen zu lösen und durch Open Source Software auch Kosteneinsparungen zu realisieren.

Die Analyse zeigt auf, welche praktischen Untersuchungen für den Einsatz von OSS gemacht wurden, wo die Chancen und der Mehrwert von OSS in der Stadtverwaltung liegen, welche Risiken und Grenzen für einen Einsatz von OSS bestehen und wie der wirtschaftliche Vergleich von OSS mit proprietärer Software ausfällt. Zusammenfassend lässt sich mit Blick auf alle Pilotprojekte festhalten, dass mit dem Einsatz von OSS-Produkten die Abhängigkeit von marktdominierenden Softwareherstellerinnen und Softwareherstellern teilweise verringert werden kann. Da aber auch OSS-Lösungen Support von Herstellerinnen und Herstellern oder anderen Vertragspartnerinnen und Vertragspartnern benötigen (sog. Subcriptions), entstehen neue Abhängigkeiten zu anderen Firmen.

Im Einzelnen resultieren die folgenden Ergebnisse aus den Pilotprojekten:

Pilotprojekt A – Basis Client
Der Ersatz der Büroarbeitsplätze aller Mitarbeitenden durch OSS-Basis Clients ist nicht möglich, da sich diese nicht in die bestehende Systemlandschaft einbinden lassen. Ein Datenaustausch mit anderen Dienststellen und externen Partnerinnen und Partnern wäre nur mit Verlusten möglich, was zu einem erhöhten Arbeitsaufwand bei der Nachbearbeitung von Dokumenten führen würde. Im Bereich der Standardfunktionalität wäre einzig die Einrichtung eines völlig isolierten Büroarbeitsplatzes möglich, was jedoch aus wirtschaftlicher Sicht keinen Sinn macht, da ein solcher nur für sehr wenige Mitarbeitende brauchbar wäre.

OSS Office-Produkte wie Libreoffice bieten nicht denselben Funktionsumfang wie die Standard Office Produkte. Für die Power User (Benutzerinnen und Benutzer mit erweiterten Funktionalitätsbedürfnissen, insbesondere bei der Software-Kategorie 1) der Stadtverwaltung müssen die Standard Office Produkte auch weiterhin angeboten werden. Der Betrieb und die Bewirtschaftung von zwei Office-Plattformen würde einen unverhältnismässig grossen personellen und finanziellen Aufwand bedeuten, was den Mehrwert nicht rechtfertigt.

Pilotprojekt B – Fachapplikationen
Die Schnittstellen von geschäftskritischen Fachapplikationen sind heute meist so konzipiert, dass sie nur mit proprietären Programmen bearbeitet werden können. Anders gesagt heisst das, dass OSS-Clients ausschliesslich in denjenigen Bereichen eingesetzt werden, in denen die Fachapplikationen auf einem Browser oder unter Citrix einwandfrei funktionieren. Bei der Beschaffung von Fachapplikationen sollte demnach darauf geachtet werden, dass sie webbasiert (also unter einem Browser lauffähig) oder virtualisiert (unter einem Citrix-Portal lauffähig) sind, damit sie auch auf einem OSS-Client genutzt werden. Zudem ist der Support durch die Herstellerfirmen sicherzustellen.

Pilotprojekt C – Groupware
In Bezug auf die Stabilität wäre OpenXchange als OSS-Lösung für Groupware eine theoretisch valable Variante. Trotzdem kommt ein Wechsel aktuell wegen der mangelnden Funktionalität nicht in Frage. Der Support für aktuelle Umsysteme wie die Integration von Mobilgeräten, Sitzungszimmern oder Call-Centern ist nicht gewährleistet, was eine Grundvoraussetzung für einen stabilen und effizienten Betrieb darstellt. Hier gilt es, die Entwicklung in den nächsten Jahren zu beobachten bzw. die Marktsituation vor der Ablösung einer bestehenden Plattform genau zu evaluieren.

Ein wichtiger Kostenfaktor sind die durch die Umstellung auf eine neue Plattform verursachten Migrationskosten. Je mehr gespeicherte Daten (Office-Dokumente, Mails, etc.) migriert werden müssten, desto höher sind diese Kosten. Wird eine Umstellung im Rahmen der regelmässigen Erneuerungen (lifecycle) durchgeführt, sind sie niedriger.

Pilotprojekt D – Virtualisierung
Zum heutigen Zeitpunkt kann eine OSS-Lösung für die Windows-Clientvirtualisierung nicht empfohlen werden. Es existiert kein Produkt, das die Anforderungen an die Desktop-Virtualisierung erfüllt. Sollte dereinst ein Ersatz des Windows-Clients ins Auge gefasst werden, würde die Auswahl an geeigneten Virtualisierungslösungen grösser. Hier gilt es demnach, die weitere Entwicklung genau zu verfolgen.

Pilotprojekt E – CMI Axioma
Da keine namhafte Einsparung von Lizenzkosten geltend gemacht werden kann, auf Kostenseite hingegen der Migrationsaufwand anfällt, würde ein Wechsel der Plattform für die Verwaltung der politischen Geschäfte aus wirtschaftlicher Sicht keinen Sinn machen. Insgesamt wäre es ein zu kleiner und unwesentlicher Schritt, um substanzielle Einsparungen oder die Verringerung der Abhängigkeit erwirken zu können.

7.2. Fazit

Mit Blick auf die strategischen Ziele der gesamtstädtischen Informatik in Bezug auf Funktionalität, Stabilität und Wirtschaftlichkeit zeigt die Potenzialanalyse auf, dass zum heutigen Zeitpunkt bei einer vollständigen Einführung von Open Source Software zum Teil beträchtliche Einschränkungen in Kauf genommen werden müssten.

Funktionalität für die Geschäftsabwicklung

In Bezug auf die Funktionalität haben die Pilotprojekte gezeigt, dass gewisse Fachapplikationen nicht mit einem OSS-Fat-Client zur Verfügung gestellt werden könnten, was den Kreis der potenziellen OSS-Anwendenden einschränkt. Weiter bietet LibreOffice für die Power User der Stadtverwaltung zu wenige Funktionalitäten an. Eine Migration der bestehenden Vorlagen und Dokumente würde eine erhebliche Investition voraussetzen. Punkto Funktionalität ist auch der erschwerte Datenaustausch mit anderen Abteilungen und externen Stellen zu erwähnen, welcher zu Fehleranfälligkeit, sinkender Produktivität und Unzufriedenheit bei den Benutzerinnen und Benutzern führen würde. Dies könnte durch die Etablierung eines herstellerunabhängigen Standard-Datenformats längerfristig gelöst werden.

Während LibreOffice für die meisten Anwendenden ein genügend guter Ersatz für Microsoft Office darstellt, fehlen bei anderen OSS-Alternativprodukten wie z.B. der Red Hat Virtualization entscheidende Funktionalitäten, die heute z.B. mit Citrix genutzt werden. Vor diesem Hintergrund kann die Virtualisierungsinfrastruktur (Citrix) heute nicht mit einem OSS-Alternativprodukt abgelöst werden.

Sicherstellen des stabilen Informatikbetriebs

In Bezug auf die Stabilität des IT-Betriebs müssten bei einem vollständigen Wechsel auf OSS-Produkte sowohl in den Wissens-Aufbau der Mitarbeitenden als auch in Supportverträge mit OSS-Firmen investiert werden. Dieser Aufwand steht in einem Zielkonflikt mit der Wirtschaftlichkeit.

Wirtschaftlichkeit

Die grösste Motivation, OSS-Produkte einzusetzen besteht darin, die Abhängigkeit von marktdominanten Herstellerinnen und Herstellern zu lösen und sich deren Diktat der Lizenzmodelle und -kosten zu entziehen. Tatsächlich fallen durch den Einsatz von OSS-Produkten die Lizenzkosten weg. Wie eingangs erwähnt, macht der Gesamtanteil der Lizenzkosten am Betrieb der IT-Infrastruktur der Stadtverwaltung rund 14 % aus. Diese Einsparung wird relativiert durch die notwendigen Supportverträge mit OSS-Fachleuten, den sogenannten Subscriptions. Insgesamt verhindern die hohen Investitionen, welche zum Aufbau der OSS-Plattformen, zum Wissensaufbau und zur Migration von Vorlagen und Dokumenten notwendig sind, damit auch über einen längeren Zeitraum einen «Return on Investment».

8. Künftige OSS-Strategie

Die Potenzialanalyse kommt zum Schluss, dass ein wirtschaftlich sinnvoller Betrieb durch einen vollständigen Umstieg auf Open Source Software heute nicht möglich ist. Vielmehr sollen die städtischen ID der Mischbetrieb bleiben, der sie bereits heute auszeichnet. Es gibt zwei Gründe für dieses Fazit. Einerseits die fehlenden Eigenschaften der Alternativen, andererseits die enge, gegenseitige Kopplung der Komponenten, die – analog eines Uhrwerks – untereinander kompatibel und aufeinander abgestimmt sein müssen. Eine ICT-Infrastruktur wie jene der Stadtverwaltung besteht aus Tausenden von Komponenten, die ineinandergreifen und korrespondieren müssen. In allen untersuchten Bereichen wurde eine enge Koppelung zwischen Applikation, Datenformat, Betriebssystem und Client-Virtualisierung festgestellt. Jede Änderung an einer Komponente beeinflusst auch die anderen. Oft ist zudem eine Applikation nur für eine bestimmte Plattform verfügbar.

Die grösste und folgenschwerste Abhängigkeit besteht in den Produkten von Microsoft Office und gerade diese können heute nicht vollständig ersetzt werden. Die Mitarbeitenden der Stadtverwaltung müssen in der Lage sein, intern und extern Dokumente auszutauschen und diese müssen auf beiden Seiten bearbeitet werden können. Will man hier den Schritt in Richtung Open Source machen und soll dies gleichzeitig verlustlos geschehen, müsste eine Ablösungsstrategie von Microsoft Office Produkten mit der Verwendung eines offenen Datenformats beginnen – konkret müsste u.a. das proprietäre DOCX-Format (Word) mit dem offenen ODT-Format ersetzt werden.

Vor diesem Hintergrund und gestützt auf den Expertenbericht kommt der Gemeinderat zum Schluss, dass es zum heutigen Zeitpunkt weder sinnvoll noch zweckmässig ist, die im Einsatz stehenden, proprietären Produkte vollständig durch OSS-Produkte abzulösen. Jedoch soll durch drei Massnahmen die Grundlage geschaffen werden, um in Zukunft noch stärker auf Open Source-Lösungen zu setzen. Zum einen, da davon auszugehen ist, dass sich die Marktsituation weiterhin ändert und in Zukunft tauglichere und kompatiblere OSS-Produkte verfügbar sein werden. Zum anderen soll OSS in den Kriterienkatalog von Beschaffungen aufgenommen werden, um Open Source stärker Rechnung zu tragen.

Massnahme 1: Bei der Beschaffung von künftigen Fachanwendungen – sei es eine Neubeschaffung oder muss eine bestehende Plattform oder Software erneuert werden (z.B, Axioma, KISS, Anazent etc.) – ist auf eine hohe Plattformunabhängigkeit zu achten. Die Digitalkonferenz erlässt hierzu Richtlinien.

Massnahme 2: Individuell entwickelte Fachanwendungen (Eigenentwicklungen) sind als OSS zu entwickeln bzw. entwickeln zu lassen; der Source Code ist im Internet zu publizieren. Die Zusammenarbeit auf Ebene Gemeinden, mit dem Kanton Bern und dem Bund wird verstärkt.

Massnahme 3: Mit der schrittweisen Etablierung von offenen Datenformaten soll die Unabhängigkeit der Stadt Bern hinsichtlich künftiger Entwicklung gestärkt werden. Die Digitalkonferenz legt dem Gemeinderat bis Ende 2020 eine Auslegeordnung mit möglichen Umsetzungsmassnahmen vor.

Antrag

Der Stadtrat nimmt den Abschlussbericht «Potenzialanalyse Open Source Software (POTOSS)» zur Kenntnis.

Bern, 30. April 2019

Der Gemeinderat

Beilage: Expertenbericht POTOSS. Potenzialanalyse OSS, Adfinis Sy Group, 23. April 2019

POTOSS
Potenzialanalyse OSS

Version 1.1
23. April 2019

Urs Amstutz (Amstutz ICT AG), Nicolas Iselin (Adfinis SyGroup AG)

Änderungskontrolle

Version	Datum	Autor	Änderung
0.1	30. November 2016		Initialer Entwurf
0.2	19. September 2017		Überarbeitung
0.3	26. September 2017		Überarbeitung
0.35	10. Juli 2018		Beschreibung Installation RHV
0.35	13. Juli 2018		Standard Tests für Crossover hinzugefügt
0.36	6. August 2018		Überarbeitung der Struktur
0.37	8. August 2018		Überarbeitung des Inhalts
0.42	12. August 2018		Überarbeitung der Struktur und Formatierung
0.46	13. August 2018		Ausarbeitung des Inhalts; Anforderungen eingefügt im Pilot C und D
0.47	17. August 2018		Testkonzept eingearbeitet
0.58	11. Dezember 2018		Mehrere Kapitel überarbeitet
0.60	14. Dezember 2018		Pilot A Tabelle vervollständigt, Text überarbeitet
0.61	24. Dezember 2018		Kapitel ausgearbeitet
0.62	26. Dezember 2018		Kapitel 2 ausgearbeitet
0.66	30. Dezember 2018		Weitere Ausarbeitung, Merge
0.69	2. Januar 2019		Weitere Ausarbeitung, Security Audit, Merge
0.71	4. Januar 2019		Weitere Ausarbeitung, Strategie (und Korrekturen daran)
0.74	22. Januar 2019		Einarbeiten Review-Feedbacks
0.76	27. Januar 2019		Einarbeiten Review-Feedbacks
0.78	2. Februar 2019		Einarbeiten Review-Feedbacks
0.81	4. Februar 2019		Einarbeiten Review-Feedbacks
0.84	10. Februar 2019		Einarbeiten Review-Feedbacks
1.0	16. April 2019		Einarbeiten Korrekturen

Version	Datum	Autor	Änderung
1.1	23. April 2019		Einarbeiten Korrekturen

Referenzierte Dokumente

Titel	Autor
One Consult Audit Bericht (2018)	Simon Gfeller (OneConsult)
Testergebnisse (.pdf) mit Unterschrift der AV (2018)	Urs Amstutz/Nicolas Iselin
Testübersicht (.xlsx) (2018)	Urs Amstutz/Nicolas Iselin
IT-Grundschutz BSI (2016)	Bundesamt für Sicherheit in der Informationstechnik Deutschland
Weisung ICT-Sicherheit für Benutzerinnen und Benutzer (2017)	Martin Müller (ID)
Client Richtlinie (2016)	Klaus Zakel (ID)

Definitionen

Begriff	Definition
AD	Siehe MS AD
API	application programming interface: Schnittstelle zur Steuerung eines Programms durch andere Programme
Authentisierung	Bei der Authentisierung beweisen Anwendende Ihre Identität (in der Regel mit Benutzendenname und Passwort)
Autorisierung	Die Autorisierung bestimmt, welche Applikationen/Funktionen bzw. Daten für Anwendende zugelassen sind. Voraussetzung ist eine erfolgreiche Authentisierung.
Citrix-Applikation	Im Bericht verwendet für Windows-Applikationen, welche bei der Stadt Bern als «einzelne» Applikationen auf dem Desktop aufgerufen und dargestellt werden, deren Ausführung aber (nach einem transparenten Login) auf einem zentralen Windows-Server erfolgt. In Tabellen mit «Citrix-App» abgekürzt.
DKMS	Dynamic Kernel Module Support: Eine Technik, die es bei Linux erlaubt, «fremde» Kernel-Module bei jedem Upgrade automatisch neu kompilieren zu lassen.
GPO	Group Policy Object
KAT1 KAT2 KAT3 KAT4	Die ID der Stadt Bern haben die Client-Applikationen in vier Kategorien eingeteilt: • KAT1: Basis-Software, ist auf jedem Desktop verfügbar • KAT2: Basis-Software, aber nur auf Bestellung verfügbar • KAT3: Fach-Applikationen, Verantwortung liegt bei den jeweiligen Direktionen. • KAT4: KAT3-Applikationen, die nur «von Hand» installiert werden können.
MDM	Mobile Device Management: Lösungen zur zentralen Verwaltung von Mobiltelefonen/Tablets: Es können Einstellungen erzwungen werden, eigene App-Stores zur Verfügung gestellt werden, verlorene Geräte auf den Fabrikzustand zurückgesetzt werden etc.
MS AD	Microsoft Active Directory: Verzeichnisdienst in einer Microsoft-Umgebung, wird (unter anderem) für die zentrale Authentisierung und Autorisierung benutzt.
OASIS	Organization for the Advancement of Structured Information Standards

Begriff	Definition
OCR	Optical Character Recognition: Es wird ein Text eingescannt und als Resultat erhält man eine editierbare Datei des Texts (zum Beispiel als Word-Dokument).
ODT	Open Document Text: Eine Variante von ODF (open document format) für Dokumente.
Ökosystem	In diesem Bericht sind digitale Ökosysteme gemeint: Das wirtschaftliche Zusammenspiel von Herstellern von Hardware, Betriebsystemen und Applikationen
RHV	Red Hat Virtualization, siehe dazu auch Pilotprojekt D (Kapitel 7)
SDK	Software Development Kit: Programmierumgebung
SSO	Single Sign On
Vendor lock in	Kundenbindung durch hohe Wechselkosten
VM	Virtuelle Maschine
Web-Applikation	Im Bericht verwendet für Applikationen, welche bei der Stadt Bern über einen Web-Browser (Chrome, Edge, Firefox, …) benutzt werden. Dies umfasst prima vista auch solche, die an einen bestimmten Browser, bestimmte Extensions und/oder an bestimmtes Betriebssystem gebunden sind.
	Weiterführendes Glossar zum Thema Open Source: http://www.bpb.de/gesellschaft/digitales/opensource/63954/glossar

Inhalt

1 MANAGEMENT SUMMARY 13
2 EINLEITUNG 15
2.1 AUFTRAG 15
2.2 GRUNDLAGEN 15
2.3 ZIELE 16
2.3.1 Pilotprojekte definieren und umsetzen 16
2.3.2 Prüfung von alternativen Software-Produkten 16
2.3.3 Entkoppelung von Fachanwendungen 16
2.3.4 Technologische Anpassungen vornehmen 16
2.3.5 Aus- und Weiterbildungen durchführen 17
2.3.6 Umsetzungsstrategie erarbeiten 17
2.4 RAHMENBEDINGUNGEN / ABGRENZUNG 17
2.5 BEGRIFFSKLÄRUNG: OSS, KOMMERZIELL 17
2.6 BETEILIGTE UND THEMENBEREICHE 18
3 METHODIK 19
3.1 BESCHREIBUNG DER PILOTPROJEKTE 19
3.2 GENERELLE ANSÄTZE 19
3.3 OSS LÖSUNGSANSÄTZE PILOT A/B 20
3.3.1 Nativ 20
3.3.2 Alternative 20
3.3.3 CrossOver 20
3.3.4 Citrix 20
3.3.5 Web-Applikation 20
3.4 LÖSUNGSANSÄTZE PILOTEN C/D/E 21
3.5 TESTKONZEPT 21
3.5.1 Testverfahren A/B 21
3.5.2 Bereitstellung der Applikationen A/B 21
3.5.3 Fehlerklassen 22
3.6 STANDARDTESTS A/B 22
3.6.1 Crossover Applikationen 22
3.6.2 Citrix-Applikationen 23
3.6.3 Web-Applikationen 23
3.7 KOSTENVERGLEICH 24

3.7.1 Lebenszyklen 24
3.7.2 Mischbetrieb 24
3.7.3 Investitionen 24
3.7.4 Betriebskosten 25
3.7.5 Indikativer Kostenvergleich 25
4 PILOTPROJEKT A: BASIS CLIENT 26
4.1 ANFORDERUNGSDEFINITION 26
4.2 UMSETZUNG 26
4.2.1 Lösungsansatz 26
4.2.2 Rollout Betriebssystem Basis Client 26
4.2.3 Exkurs: Vergleich zentrale Steuerung Clients 27
4.2.4 Client Einstellungen 27
4.2.5 Konfiguration Infrastruktur 31
4.2.6 Funktionstest 32
4.2.7 Security 34
4.3 TESTDURCHFÜHRUNG 35
4.3.1 Grundsätzliches 35
4.3.2 Testfälle/Ergebnisse pro Applikation 36
4.4 MIGRATIONSZENARIO AUF OSS 47
4.4.1 Erfüllung der Anforderungen 47
4.4.2 Auswirkungen auf den IT Betrieb 47
4.4.3 Vendor Lock In 47
4.5 KOSTENVERGLEICH 48
4.5.1 Szenario 48
4.5.2 Investitionen 48
4.5.3 Betriebskosten 49
4.6 ZUSAMMENFASSUNG 50
4.6.1 Ergebnisse 50
4.6.2 Chancen 51
4.6.3 Risiken 51
4.6.4 Finanzen 51
4.6.5 Empfehlung 51
4.6.6 Übersicht 52
5 PILOTPROJEKT B: FACHAPPLIKATIONEN 53
5.1 ANFORDERUNGSDEFINITION 53

5.2 UMSETZUNG 53
5.2.1 Lösungsansatz 53
5.2.2 Aufbau der Infrastruktur 53
5.2.3 Installation Basis-Client 54
5.2.4 Installation der Applikationen 54
5.2.5 Bereitstellen der Daten 55
5.2.6 Konfiguration Infrastruktur 55
5.2.7 Funktionstest 55
5.3 TESTDURCHFÜHRUNG 55
5.3.1 Grundsätzliche Lösungsansätze 55
5.3.2 Native, Alternative, Crossover, Citrix-Applikation 55
5.3.3 Testfälle pro Applikation 55
5.4 MIGRATIONSZENARIO AUF OSS 68
5.4.1 Erfüllung der Anforderungen 68
5.4.2 Auswirkungen auf den IT Betrieb (gleich wie Pilot A) 68
5.4.3 Vendor Lock In 68
5.5 KOSTENVERGLEICH 69
5.5.1 Szenario 69
5.5.2 Investitionen 69
5.5.3 Betriebskosten 69
5.6 ZUSAMMENFASSUNG 70
5.6.1 Ergebnisse 70
5.6.2 Chancen 70
5.6.3 Risiken 70
5.6.4 Finanzen 70
5.6.5 Empfehlung 70
5.6.6 Übersicht 70
6 PILOTPROJEKT C: GROUPWARE 72
6.1 ANFORDERUNGSDEFINITION 72
6.2 UMSETZUNG 72
6.2.1 Lösungsansatz 72
6.2.2 Aufbau der Infrastruktur 72
6.2.3 Installation der "Applikationen" 73
6.2.4 Bereitstellen der Test-Daten 73
6.2.5 Anbindung der Schnittstellen 73

6.2.6 Funktionstest ... 74
6.3 TESTDURCHFÜHRUNG ... 74
6.3.1 Testfälle / Ergebnisse ... 74
6.4 MIGRATIONSZENARIO AUF OSS PRODUKTE ... 78
6.4.1 Erfüllung der Anforderungen ... 79
6.4.2 Auswirkungen auf den IT Betrieb ... 79
6.4.3 Vendor Lock-In ... 80
6.5 KOSTENVERGLEICH ... 80
6.5.1 Szenario ... 80
6.5.2 Investitionen ... 80
6.5.3 Betriebskosten ... 81
6.6 ZUSAMMENFASSUNG ... 82
6.6.1 Ergebnisse ... 82
6.6.2 Chancen ... 82
6.6.3 Risiken ... 82
6.6.4 Finanzen ... 82
6.6.5 Empfehlung ... 83
6.6.6 Übersicht ... 83
7 PILOTPROJEKT D: CLIENT VIRTUALISIERUNG ... 84
7.1 ANFORDERUNGSDEFINITION ... 84
7.2 UMSETZUNG ... 84
7.2.1 Lösungsansatz ... 84
7.2.2 Aufbau der Infrastruktur ... 85
7.2.3 Installation RedHat Virtualization Manager ... 85
7.2.4 Installation einer VM ... 85
7.2.5 Bereitstellen der Test-Daten ... 85
7.2.6 Anbindung der Schnittstellen ... 85
7.2.7 Konfigurationen ... 85
7.2.8 Funktionstest ... 86
7.3 TESTDURCHFÜHRUNG ... 86
7.3.1 Testfälle ... 86
7.4 MIGRATIONSZENARIO AUF OSS ... 94
7.4.1 Erfüllung der Anforderungen ... 94
7.4.2 Auswirkungen auf den IT Betrieb ... 94
7.4.3 Vendor Lock In ... 95

7.5 KOSTENVERGLEICH 95
7.5.1 Szenario 95
7.5.2 Investitionen 95
7.5.3 Betriebskosten 96
7.6 ZUSAMMENFASSUNG 97
7.6.1 Ergebnisse 97
7.6.2 Chancen 97
7.6.3 Risiken 97
7.6.4 Finanzen 97
7.6.5 Empfehlung 97
7.6.6 Übersicht 98
8 PILOTPROJEKT E: CMI AXIOMA 99
8.1 ANFORDERUNGSDEFINITION 99
8.2 UMSETZUNG 99
8.2.1 Lösungsansatz 99
8.2.2 Aufbau der Infrastruktur 99
8.2.3 Installation der Applikation 99
8.2.4 Bereitstellen der Testdaten 99
8.2.5 Konfigurationen 100
8.2.6 Funktionstest 100
8.3 TESTDURCHFÜHRUNG 100
8.3.1 Testfälle 100
8.4 MIGRATIONSZENARIO AUF OSS 101
8.4.1 Erfüllung der Anforderungen 101
8.4.2 Auswirkungen auf den IT Betrieb 101
8.4.3 Benutzendenschulungen 101
8.4.4 Vendor Lock In 101
8.5 KOSTENVERGLEICH 101
8.5.1 Szenario 101
8.5.2 Investitionen 101
8.5.3 Betriebskosten 102
8.6 ZUSAMMENFASSUNG 103
8.6.1 Ergebnisse 103
8.6.2 Chancen 103
8.6.3 Risiken 103

8.6.4 Finanzen 103
8.6.5 Empfehlung 103
8.6.6 Übersicht 104
9 STRATEGISCHE ASPEKTE 105
9.1 URSACHENANALYSE 105
9.1.1 Fehlende Eigenschaften der Alternativen 105
9.1.2 Enge Kopplung 105
9.2 STRATEGIEN 105
9.2.1 Fehlende Eigenschaften 105
9.2.2 Enge Kopplung 106
9.2.3 Massnahmen 108

1 Management Summary

Gibt es eine Alternative zu den grossen Softwareherstellern? Diese Frage taucht immer wieder dann auf, wenn Softwarelizenzen zu hohen Kosten neu beschafft werden müssen.

Die marktdominanten Softwarehersteller verfügen faktisch über ein Monopol. Beispielsweise sind auf ca. 90% der Büroarbeitsplätze Microsoft Windows in den verschiedenen Versionen installiert. Bei der Büroautomatisation macht der Anteil von Microsoft Office mehr als 70% aus. Somit herrscht kein wirklicher Wettbewerb und die Anbieter haben eine grosse Freiheit in der Preisgestaltung.

Eine Alternative ist Open Source Software (OSS). Der Grundgedanke besteht darin, dass eine weltumspannende Gruppe von Entwicklern Beiträge an ein gemeinsames Softwareprodukt leisten, und dieses im Gegenzug dann kostenlos nutzen können. Die Nutzung von Open Source Software verursacht keine Lizenzkosten, was auf den ersten Blick, insbesondere im Vergleich zu den hohen Lizenzkosten proprietärer Software, verlockt.

Vor diesem Hintergrund hat der Stadtrat den Auftrag erteilt, die Einsatzmöglichkeiten von Open Source Software in der Stadtverwaltung Bern zu überprüfen. Dabei soll eine detaillierte Ablösungsstrategie von Microsoft- und CITRIX-Produkten erarbeiten werden und anhand von konkreten Pilotprojekten die technische Machbarkeit und die Grenzen eines Einsatzes von OSS Produkten untersucht werden.

Die Informatikdienste der Stadt Bern wurden beauftragt, mit dem Projekt POTOSS eine Potenzialanalyse anhand von vorgegebenen konkreten Pilotprojekten für den Einsatz von Open Source Software zu erarbeiten.

Die vorliegende Potenzialanalyse ist das Ergebnis des Projekts POTOSS und zeigt auf:

- Welche praktischen Untersuchungen für den Einsatz von Open Source Software gemacht wurden
- Wo die Chancen und der Mehrwert eines Einsatzes von Open Source Software in der Verwaltung der Stadt Bern liegen
- Welche Risiken oder Grenzen für einen Einsatz von Open Source Software bestehen
- Wie der wirtschaftliche Vergleich von OSS mit proprietärer Software ausfällt
- Welche konkreten Empfehlungen für das weitere Vorgehen bzw. die Strategie resultieren

Die Potenzialanalyse stützt sich auf die durchgeführten Pilotprojekte ab. Jedes Pilotprojekt wird beschrieben mit Zielsetzungen und Rahmenbedingungen, Erkenntnissen und Empfehlungen.

Die Erkenntnisse können wie folgt zusammengefasst werden:

- Im Bereich der Standardfunktionalität eines Bürorarbeitsplatzes deckt Open Source Software einen grossen Teil der Bedürfnisse vieler Benutzenden ab
- Der Datenaustausch mit anderen Dienststellen und externen Partnern ist nur mit Verlusten möglich. Dies führt zu erhöhtem Arbeitsaufwand bei der Nachbearbeitung von Dokumenten
- Die Schnittstellen von geschäftskritischen Applikationen sind meist so konzipiert, dass sie nur mit proprietären Programmen bearbeitet werden können
- Die OSS Office Produkte (LibreOffice) bieten nicht ganz denselben Funktionsumfang wie die Microsoft Office Produkte. Inwieweit dadurch die Arbeitsprozesse der Stadt Bern tangiert werden hängt sehr stark vom Einzelfall ab. Für gewisse Power User müssen die Microsoft Office Produkte weiterhin angeboten werden
- Ein Teil der Fachapplikationen, welche nicht virtualisiert (Citrix) oder als WEB Applikation angeboten werden, können nur über eine bestehende Windows Plattform zur Verfügung gestellt werden
- Durch das Angebot zweier Plattformen anstelle einer für das Angebot der für die Geschäftstätigkeit benötigten Funktionalität steigen die Kosten für den IT Betrieb
- Obwohl die Lizenzkosten isoliert betrachtet sehr hoch sind, machen Sie nur einen kleinen Prozentsatz der gesamten Kosten eines professionellen IT Betriebs aus

- Der Kostenvorteil durch den Wegfall von Lizenzkosten wird durch die Notwendigkeit eines Parallelbetriebs zweier Plattformen wieder relativiert
- Mit dem Einsatz von OSS Produkten kann die Abhängigkeit von marktdominierenden Softwareherstellern teilweise gelockert werden
- Für den Support von OSS Produkten ist man auf die Zusammenarbeit mit OSS-Firmen angewiesen. Dadurch entstehen neue Abhängigkeiten zu anderen Firmen, dieses sind aber in der Regel schwächer, weil keiner der Anbieter ein exklusives Recht an der Software hat.

Während Libreoffice für die meisten Anwendenden ein genügend guter Ersatz für Microsoft Office darstellt, fehlen bei anderen OSS Alternativprodukten wie z.B. RHV entscheidende Funktionalitäten die heute z.B. mit Citrix genutzt werden. In diesem Fall kann die Virtualisierungsinfrastruktur (Citrix) nicht mit einem OSS Alternativprodukt abgelöst werden.

Die ID der Stadt Bern haben den Auftrag, die Informatikinfrastruktur wirtschaftlich zu betreiben. OSS Produkte verursachen keine Lizenzkosten. Für die Sicherstellung des Betriebs müssen jedoch bei Firmen, welche sich auf OSS spezialisiert haben, "Subscriptions" für den Support abgeschlossen werden, welche das Einsparpotenzial durch die wegfallenden Lizenzkosten wieder zunichte machen.

Zum heutigen Zeitpunkt ist es nicht möglich, z.B. die bestehende Client Plattform durch OSS Produkte vollständig abzulösen. Aus diesem Grund wird für einen Teil der Mitarbeitenden die bestehende Plattform erhalten bleiben müssen. Der Betrieb von zwei, anstelle von einer Plattform verursacht höhere Kosten als bisher.

Insgesamt macht der Anteil der Lizenzkosten am Betrieb der IT Infrastruktur der Stadt Bern lediglich ca. 14% aus. Eine Einsparung der Lizenzkosten durch OSS ist somit marginal.

Die Abhängigkeit von marktdominanten Herstellern ist stärker durch die Datenformate als den Applikationen gegeben. Die Mitarbeitenden der Stadt Bern tauschen intern oder extern Dokumente aus, die auf beiden Seiten bearbeitet werden. Damit dies verlustlos geschehen kann, muss eine Ablösungsstrategie von Microsoft Office Produkten mit der Verwendung eines offenen Datenformats beginnen.

2 Einleitung

2.1 Auftrag

Mit Ziffer 4 des SRB 2015-494 vom 12. November 2015 hat der Stadtrat folgenden Auftrag an den Gemeinderat erteilt:

> *"Der Gemeinderat wird beauftragt, bis Ende 2017 zu Handen des Stadtrats eine detaillierte Ablösungsstrategie von Microsoft- und CITRIX-Produkten zu erarbeiten. CLIMB wird abgestimmt auf diese Strategie, die darauf abzielt, bestehende Abhängigkeiten zu reduzieren. Die Ablösungsstrategie wird mittels Pilotprojekten, Prüfung von Alternativen, Entkoppelung von Fachanwendungen, technologischen Anpassungen und Weiterbildungen erarbeitet. Für die Erstellung der Ablösungsstrategie beantragt der Gemeinderat bis Ende Februar 2016 beim Stadtrat einen angemessenen Projektierungskredit"*

2.2 Grundlagen

Die elementare Grundlage für das Projekt POTOSS bildet der vorgängig zitierte Auftrag des Stadtrats an die Informatikdienste der Stadt Bern.

Die Informatikdienste der Stadt Bern (ID) betreiben Arbeitsplätze und die Applikationen für die Mitarbeitenden der Stadtverwaltung Bern und der städtischen Volksschulen. Zusätzlich zu den ca. 180 Fachapplikationen der Stadtverwaltung, welche sehr spezialisiert auf die Bedürfnisse von bestimmten Arbeitsabläufen zugeschnitten sind, setzt die ID auf bekannte und verbreitete Lösungen wie, z.B. die Office Suite von Microsoft oder die Virtualiserungsplattform von Citrix. Dementsprechend verfügen die Mitarbeitenden der ID über ein profundes Know-how zu diesen Lösungen, jedoch nur punktuell über OSS Alternativprodukte.

Um eine objektive Sicht zum Angebot an OSS Lösungen zu erhalten und um auf konkrete Betriebserfahrungen zugreifen zu können, hat die ID eine Ausschreibung für das Projekt POTOSS gemacht. Ausgeschrieben wurden:

1. Die Realisierung der Pilotprojekte und technische Beratung über OSS Applikationen
2. Projektmanagement und Einbringen der Kenntnis über die Applikationen der Stadt Bern

In der Schweiz gibt es nur eine überschaubare Anzahl potentieller Anbieter für diese Leistungen. Nach der Ausschreibung ist nur ein Angebot der Firma Adfinis SyGroup AG für die Realisierung der Pilotprojekte eingegangen.

Als professionelle Betreiberin einer komplexen IT Infrastruktur verfügen die ID der Stadt Bern über Systeme, welche als Grundlage die Inventarinformationen für das Projekt POTOSS lieferten. Dies umfasste folgende Aspekte:

- Bestandesinformation über die Anwendenden
- Inventarinformationen über eingesetzte Hardware
- Inventarinformationen über zugewiesene Software

Dadurch war erkennbar, welche Applikationen welchen Anwendenden zugewiesen wurde, jedoch war nicht ersichtlich, ob und wie intensiv die Anwendungen tatsächlich genutzt wurden (fehlendes Software Metering).

Die Informatikdienste der Stadt Bern verfügen über Richtlinien und Vorgaben für den IT Betrieb, insbesondere auch hinsichtlich Betriebssicherheit (ICT Security). Basierend darauf wurde ein Security Audit mit dem OSS Client durchgeführt.

Über das Thema OSS sind verschiedene Publikationen öffentlich verfügbar. Selbstverständlich bildeten diese auch eine wertvolle Grundlage für die vorliegende Studie. Wenn z.B. aus vertrauenswürdigen Quellen offensichtlich war, dass für die eine oder andere Lösung eine OSS Variante technisch nicht

funktionsfähig ist, wurde in einzelnen Fällen auf das Nachvollziehen in Form von Tests in den Pilotprojekten verzichtet.

Zu guter Letzt bildet das Know-how und die Erfahrung der Spezialisten von Adfinis SyGroup AG aus vergleichbaren Kundensituationen die wichtigste Grundlage für diese Studie. Dabei konnte auf praktische Erfahrung mit namhaften, teilweise auch grossen Firmen und Organisationen zurückgegriffen werden.

2.3 Ziele

2.3.1 Pilotprojekte definieren und umsetzen

Die Machbarkeit eines Einsatzes von OSS Produkten in der Stadt Bern soll realitätsnah untersucht werden. Dazu wurden bereits im Rahmen der Ausschreibung fünf Pilotprojekte und deren Zielsetzungen ausgearbeitet. Sie sind nachstehend aufgelistet:

- Pilot A: Basis Client
- Pilot B: Fachapplikationen
- Pilot C: Groupware
- Pilot D: Virtualisierung
- Pilot E: CMI AXIOMA

In Kapitel 3.1 sind die Pilotprojekte im Detail beschrieben.

Zu Beginn des Projekts POTOSS entschied der Projektausschuss (PAS), dass die Pilotprojekte im Betriebsumfeld der Stadt Bern aufzubauen sind. Dieser Entscheid führte zu wesentlich realitätsnäheren Erkenntnissen, als ein Aufbau der Pilotprojekte in einer "Laborumgebung", wie dies ursprünglich vorgesehen war.

Das Pilotprojekt C umfasst den Test einer OSS Alternative für die Groupware Lösungen. Zu Beginn des Pilotprojekts erkannte das Projektteam, dass die Integration der Smartphones und Tablets in die Groupware Lösung, obwohl nicht explizit in der Potenzialanalyse gefordert, ein ausschlaggebendes Entscheidkriterium für eine OSS Alternative darstellt. Am Projektausschuss wurde deshalb eine Erweiterung des Umfangs des Pilotprojekts C um die MDM Betriebslösung beantragt, was durch den Projektausschuss bewilligt wurde.

2.3.2 Prüfung von alternativen Software-Produkten

Die Prüfung von alternativen Softwareprodukten wurde für alle Pilotprojekte (ausser E) durchgeführt. Dies war insbesondere für die Applikationen mit verbreiteter Anwendung, wie z.B. im Pilotprojekt A (Basis Client) möglich. Im Pilotprojekt B (Fachapplikationen) fanden sich keine echten OSS Alternativen mit vergleichbarer Funktionalität wie die bisher eingesetzten proprietären Fachapplikationen.

2.3.3 Entkoppelung von Fachanwendungen

Die Fachanwendungen wurden bereits bei der letzten Client Migration im Rahmen des Projekts CLIMB auf applikatorischer Ebene durch weitestgehende «Applikations-Virtualisierung» vom proprietären Betriebssystem des Clients entkoppelt. Es galt zu prüfen, wie gut diese Applikationen auch auf einem OSS-Client funktionieren.

2.3.4 Technologische Anpassungen vornehmen

Der Auftrag "Potenzialanalyse" umfasst im eigentlichen Wortsinn die Untersuchung, inwieweit es möglich ist, die bestehende Software durch Open Source Software abzulösen. Im Rahmen der Pilotprojekte wurden alle technologischen Anpassungen / Erweiterungen an der bestehenden Infrastruktur

vorgenommen, die notwendig waren, um die in der Potenzialanalyse geforderten Erkenntnisse zu gewinnen.

2.3.5 Aus- und Weiterbildungen durchführen

Gemäss Auftrag wurde ein Teil des Budgets dafür vorgesehen, Ausbildungen durchzuführen, damit die Spezialisten der ID zu den Pilotprojekten beitragen können. Die Praxis der Zusammenarbeit mit den Spezialisten der ID der Stadt Bern hat gezeigt, dass keine "Ausbildung" im eigentlichen Sinn erforderlich war, sondern durch "learning by doing" im Rahmen der Pilotprojekte der praxisorientierteste und der effektivste Weg der Wissensvermittlung gefunden wurde.

2.3.6 Umsetzungsstrategie erarbeiten

Die Strategie für einen erfolgreichen Einsatz von Open Source Software wird im Kapitel 10 dargelegt. Die Umsetzung der technischen Plattformen ist in den Pilotprojekten erfolgt.

Ziel war auch die Schaffung von Transparenz, indem die Szenarien mit vergleichbaren Praxisbeispielen von erfolgreich umgesetzten Vorhaben belegt werden.

2.4 Rahmenbedingungen / Abgrenzung

Die Potenzialanalyse untersucht die Möglichkeiten für einen weitergehenden Einsatz von Open Source Software bei den Informatikdiensten der Stadt Bern. Das Projekt ist wie folgt abgegrenzt:

- Die bestehende ICT-Infrastruktur wird durch die vorgesehenen Pilotprojekte nicht tangiert. Der Betrieb der heutigen ICT-Systemlandschaft ist dauernd sichergestellt.
- Die definierten Pilotprojekte orientieren sich funktional an einzelnen bestehenden Anwendungen, ersetzen sie jedoch im Rahmen dieser Potenzialanalyse nicht.
- Ziel ist es, den Teil der bestehenden Applikationen mit der möglichst grössten Wirkung zu prüfen. Aus diesem Grund wurden Fachapplikationen, welche von weniger als fünf (1-4) Personen eingesetzt werden, nicht weiter untersucht.
- Untersucht wird das Potenzial für den Einsatz von OSS in der ID der Stadt Bern durch Pilotprojekte im realen Betriebsumfeld. Im Rahmen des Projekts wird die ICT Infrastruktur nicht dauerhaft verändert.
- Die Pilotprojekte dienen somit als "proof of concept" und wurden nicht zu vollständigen Betriebslösungen ausgebaut
- Die Kostenvorteile werden als Schätzung dargestellt. Eine genauere Berechnung erzeugt eine Scheingenauigkeit, die nicht sinnvoll ist.

2.5 Begriffsklärung: OSS, kommerziell

Bei der Diskussion um Open Source Software werden verschiedene Begriffe immer wieder miteinander verwechselt. Hier kurz die wichtigesten Definitionen:

OSS (open source software): Software, deren Quellcode offengelegt ist. Heutzutage bedeutet das meist, dass der Quelltext öffentlich zum Download bereitgestellt wird. Diese Software untersteht gewissen Lizenzbedingungen. Es gibt verschiedene OSS Lizenzen welche den Anwendenden unterschiedliche Rechte und Pflichten einräumen. Das Recht auf eine beliebige Nutzung wird praktisch bei allen OSS Lizenzen eingeräumt. Die Lizenz kostet in der Regel nichts, aber man muss sich daran halten, solange man die Software nutzt.

CSS (closed source software): Nur die Autoren der Software haben Zugang zum Quellcode, angeboten wird normalerweise lediglich eine kompilierte Version. Anwendende können also weder die Software im Detail untersuchen noch anpassen. Auch für diese Software gibt es eine Lizenz, diese ist aber in der Regel kostenpflichtig, räumt als einziges Recht die Benutzung der Software von einer Anzahl Benutzenden ein und verbietet jede Art von Analyse / Reverse Engineering der Software. Früher galten

diese Lizenzen für eine bestimmte Version einer Software «für immer», in den letzten Jahren wurde diese Lizenzierung immer häufiger ersetzt durch Abo-Modelle, wo man die Lizenz zwar für alle Versionen (auch künftige) erwirbt, dafür nur für eine beschränkte Zeit – man bezahlt «Jahresgebühren». Je nach Lizenz erhält man auch Support, das heisst man erhält bei technischen Problemen Unterstützung.

Das Geschäftsmodell von closed source-Firmen beruht auf strenger Geheimhaltung des Source Codes und dem Verkauf von **Software-Lizenzen**.

Open source-Firmen verdienen ihr Geld nicht mit Software-Lizenzen (da diese in der Regel kostenlos sind), sondern mit sogenannten **Subscriptions**. Mit einer Subscription wird nicht die Berechtigung zur Benutzung (diese wird schon durch die kostenlose Lizenz eingeräumt), sondern die Berechtigung für Support erworben.

Aus Sicht des Kunden mag der Unterschied zwischen Lizenz und Subscription irrelevant sein (schliesslich bezahlt man einen bestimmten Betrag für die Benutzung einer Software), aber diese Unterscheidung hat doch einige interessante Konsequenzen:

- Closed Source Software kann nur vom Hersteller repariert werden, open source Software von allen, die den Source Code verstehen. Aus diesem Grund können auch mehrere, völlig voneinander unabhängige Firmen Subscriptions anbieten.
- Mit Subscriptions ist auch für open source Firmen ein nachhaltiges Geschäftsmodell möglich. Bekanntestes Beispiel ist Red Hat mit ca 10'000 Angestellten, aber auch schon Open Xchange AG (siehe später im Pilot C) beschäftigt ca 200 Angestellte.

2.6 Beteiligte und Themenbereiche

Die Potenzialanalyse wurde in Zusammenarbeit mit den Mitarbeitenden der Informatikdienste der Stadt Bern und den Applikationsverantwortlichen der Fachabteilungen erstellt.

Die Spezialisten der Informatikdienste der Stadt Bern waren beim Aufbau der Infrastruktur massgeblich beteiligt.

Die Mitarbeitenden der Fachabteilungen wurden eingeladen, um die Fachapplikationen unter den OSS Linux Client zu testen und zu beurteilen, ob diese den Anforderungen aus dem Betrieb genügen.

3 Methodik

3.1 Beschreibung der Pilotprojekte

Von den Informatikdiensten der Stadt Bern wurde früh erkannt, dass nicht nur das Benutzenden-Erlebnis, sondern auch die Betreibbarkeit der Lösungen untersucht werden muss.

Der Projektausschuss hat entschieden, die Pilotprojekte auf der Infrastruktur der Informatikdienste der Stadt Bern und nicht in Laborumgebungen durchzuführen. Es besteht der Anspruch, dass

- Die konkrete Situation der ID der Stadt Bern betrachtet wird
- Die Pilotprojekte integriert in die Infrastruktur der ID der Stadt Bern durchgeführt werden
- Die Betriebsaspekte mitberücksichtigt werden

Folgende Pilotprojekte wurden durchgeführt:

Pilotprojekt A: Entwicklung eines OSS-Clients im Umfang des bestehenden Windows-Clients mit den Software-Produkten der Kategorie 1 und 2. Dabei sollen die proprietären Software-Produkte, wo sinnvoll und machbar, durch Open Source Produkte ersetzt werden.

Es wurde ein OSS Client (basierend auf SUSE) und eine Plattform für den automatischen Rollout von Clients aufgebaut. Die Applikationen aus dem Software-Inventar wurden wo möglich durch OSS-Alternativen ersetzt, ansonsten via Citrix genutzt und/oder mit Crossover paketiert und zur Verfügung gestellt.

Pilotprojekt B: Installieren und testen der Fachanwendungen aus der Software-Kategorien 3 auf dem entwickelten OSS-Client gemäss Punkt 1.

Es wurden alle KAT3-Applikationen die von mehr als vier Benutzenden eingesetzt werden, aus dem Software-Inventar auf dem Client bereitgestellt und zusammen mit den Applikationsverantwortlichen getestet.

Pilotprojekt C: Aufbau einer OSS-Plattform für die Services Mail, Kalender, Ressourcen-, Aufgaben- und Notizenverwaltung, als Alternative zu MS Outlook und MS Exchange.

Gegenüber der ursprünglichen Zielsetzung hat das Projektteam beantragt, dass für das Pilotprojekt C die Betriebsanforderungen berücksichtigt werden sollen (Redundanz, Failover etc.).

Pilotprojekt D: Aufbau einer OSS-Plattform für die Applikations- und Client-Virtualisierung als Alternative zur bestehenden Citrix-Plattform und Einbindung von bereits virtualisierten Produkten der Software-Kategorien 1, 2 und 3.

Es wurde eine OSS-Virtualisierungsplattform aufgebaut. Zum Zeitpunkt des Variantenentscheids gab es noch keine OSS Lösungen, die speziell für die (Windows-) Clientvirtualisierung optimiert waren. Es wurde (im Wissen um dieses Defizit) eine Lösung auf Basis von RHV (Redhat Enterprise Virtualisation) implementiert.

Pilotprojekt E: Serverseitige Implementierung der Fachanwendung CMI Axioma (Geschäftsverwaltung) auf einer OSS-Plattform.

Nachdem mit dem Hersteller der Software die Strategie und die möglichen Ansätze für eine Open Source Lösung erörtert wurde, musste der Umfang des Pilotprojekts angepasst werden. Anstelle einer Ersatzlösung kam nur eine Portierung der Datenbank in Frage.

3.2 Generelle Ansätze

- Trotz frühen negativen Erkenntnissen wurden die Pilotprojekte in der Praxis umgesetzt. Beispiele:
    - Kein Herstellersupport bei Crossover (Betriebsverhindernd)

  - Kein Herstellersupport vom aktuellen MDM-System für ein OSS Groupware-System
  - Der Hersteller von CMI AXIOMA hat zur Zeit keine OSS Strategie
- Wenn die Aussagen zu den Themen klar war:
  - Aussagen von vergleichbaren oder grösseren Systemen als Erkenntnis akzeptiert und im Test nicht nachvollzogen
  - Der Aufwand für die Umsetzung der Piloten wurde pro Applikation limitiert

3.3 OSS Lösungsansätze Pilot A/B

3.3.1 Nativ

In diesem Fall wird eine Applikation durch das gleichnamige OSS Produkt des gleichen Herstellers ersetzt. Hier stellt sich die Frage, ob der volle Funktionsumfang in der Linux Variante implementiert ist. Es wird vorausgesetzt, dass die implementierten Funktionen fehlerfrei sind. Methodisch wird ein "Desk research“ durchgeführt, mit dem der Funktionsumfang der Linux Variante mit demjenigen der Windows Applikation verglichen wird. Fehlen nach Beurteilung durch die Anwendungsverantwortlichen entscheidende Funktionen, ist das Testergebnis "betriebseinschränkend" oder sogar "betriebsverhindernd".

3.3.2 Alternative

Eine OSS Alternative bietet vergleichbare Funktionalitäten wie die Windows Applikation. Die Herausforderung besteht darin, mit Funktionalitätstests zu ermitteln, ob die OSS Alternative den vollen Funktionsumfang anbietet, der für die betrieblichen Aufgaben der Mitarbeitenden der Stadt Bern benötigt wird. Hier sind die Anwendungsverantwortlichen gefordert, die betriebsnotwendigen Testfälle aufzustellen und diese im Anschluss vollständig durchzutesten.

3.3.3 CrossOver

Die originale Windows Applikation wird auf Linux installiert. Dies ist technisch nur mit Hilfe einer zusätzlichen Zwischenschicht (Crossover) möglich. Crossover emuliert gegenüber der Applikation ein Windows-System. Die Funktionalität der Applikation bleibt somit unverändert und wird nicht getestet. Im Zusammenhang mit den Schnittstellen oder der Bildschirmdarstellung gibt es jedoch eine Anzahl typischer Testfälle, die geprüft werden müssen. Diese grundlegenden Testfälle sind für alle Crossover Applikationen gleich und werden um spezielle Testfälle der Applikationsverantwortlichen ergänzt. Weiter werden bei einer Umsetzung mit Crossover sämtliche Hilfsprogramme (wie Java, .NET, etc) mit in das Software-Paket integriert, ob dies vollständig gelungen ist muss mit spezifischen Tests in Absprache mit den Applikationsverantwortlichen verifiziert werden.

3.3.4 Citrix

Durch die Umstellung von FAT auf THIN Clients im Rahmen des Projekts CLIMB wurde ein grosser Anteil der Applikationen virtualisiert. In diesem Fall wird die Applikation auf einem zentralen Server ausgeführt und auf dem OSS Client durch den Citrix Receiver dargestellt. Die Applikationen werden aus dem (internen) Portal gestartet. Bei diesen Applikationen wird geprüft, ob sie gestartet werden können und ein Einloggen möglich ist. Der Funktionalitätsumfang ist unverändert und wird nicht getestet.

3.3.5 Web-Applikation

In diesem Fall wird die Applikation auf einem entfernten Server ausgeführt und auf dem OSS Client durch den Browser dargestellt. Hier wird geprüft, ob die Applikation gestartet werden kann und ein Einloggen möglich ist. Der Funktionalitätsumfang ist unverändert und wird nur rudimentär getestet. Heikel sind Applikationen, die zwar im Browser laufen, aber zusätzlich direkte Abhängigkeiten vom Web-Browser (z.B. „läuft nur mit Microsoft Internet Explorer“) oder sogar vom darunterliegenden Betriebssystem (z.B. „läuft nur auf Windows“) haben.

3.4 Lösungsansätze Piloten C/D/E

Pilot C: Neben dem redundanten Aufbau der Groupeware-Lösung und einer Test-Integration mit der MDM-Lösung der Stadt Bern wurde nur der Web-Client geprüft.

Pilot D: Es war zu Beginn des Projekts klar, dass es keine verbreitete OSS-Virtualisierungs-Lösung mit Support für Windows-Applikationsvirtualisierung klar. Es wurde entschieden, einen Prototypen aufzubauen und zu bewerten.

Pilot E: Nach ersten Abklärungen mit dem Hersteller war klar, dass der Hersteller zur damaligen Zeit kein Interesse daran hatte, eine wie im Auftrag beschriebene Umsetzung ins Support-Portfolio aufzunehmen. Es wurde entschieden, den Auftrag wenigstens «so weit wie möglich» umzusetzen.

3.5 Testkonzept

Die Testvorgaben und die Beurteilung der Testergebnisse wurden durch die Applikationsverantwortlichen der Fachbereiche vorgenommen.

3.5.1 Testverfahren A/B

Für die Kategorie "Native" OSS Applikationen hat Adfinis SyGroup Lösungen vorgeschlagen und mit Hilfe eines "desk research“ den Funktionsumfang des OSS Produkts im Vergleich zum Windows Produkt überprüft.

Die Tests der Kategorie "Alternative" wurden bei der ID der Stadt Bern in einem dafür eingerichteten Testraum mit sechs Clients durchgeführt (Vier Desktops und zwei Notebooks).

Die Tests werden durch die Applikationsverantwortlichen der jeweiligen Applikationen durchgeführt. Diese sind in der Softwareliste aufgeführt. Die Tests werden durch einen Spezialisten der Adfinis SyGroup begleitet, um die Tests möglichst effizient durchzuführen und zu einem aussagekräftigen Ergebnis zu kommen. Gegebenenfalls werden die Testfälle ad hoc ergänzt. Die Testdauer beträgt im Durchschnitt etwa 4h.

Die Tests der Kategorie "Crossover", "Citrix-" und WEB Applikationen erfordern, vereinfacht ausgedrückt, ein Aufstarten und Login in die entsprechende Applikation. Dies muss von einem Linux Client ausgeführt werden. Die Login Credentials stehen nur den Applikationsberechtigten zur Verfügung. Die Testdauer beträgt pro Applikation ca. 30 Min.

3.5.2 Bereitstellung der Applikationen A/B

Basis für die Installation der Applikationen ist die Softwareliste der Stadt Bern. Wie oben in 3.2 beschrieben, kann eine Applikation auf technisch verschiedene Möglichkeiten ausgeführt werden. Je einfacher eine Implementation technisch ist, desto besser – vorausgesetzt die Benutzendenanforderungen werden erfüllt. Die folgende Liste beginnt mit der „besten“ Implementation und es folgt dann die jeweils schlechtere:

nativ: Dieselbe Applikation existiert auch unter Linux und kann deshalb direkt aus den Paketquellen installiert werden. Beispiel: 7-zip

Alternative: Es gibt eine Alternative, welche die Funktionalität für die meisten Use-Cases abdeckt. Diese kann ebenfalls direkt aus den Paketquellen installiert werden. Beispiel: Firefox (anstelle von Microsoft Internet Explorer).

CrossOver: Die originale Windows-Applikation wird lokal mit der Windows-Emulationsschicht CrossOver (kostenpflichtige Version von WINE von CodeWeavers) installiert und so genutzt. Beispiel: Banana Buchhaltung.

Citrix-Applikation: Die Applikation wird remote auf einem Windows Server ausgeführt und wird von dort mit dem Citrix Receiver lokal dargestellt: Beispiel: MS Project.

Auf der Liste der Kat1/Kat2-Software sind total 38 zu installierende Software-Pakete (das sind weniger als die Anzahl Applikationen, da insbesondere Microsoft Office für die Tests in einzelne Applikationen unterteilt wurde).

Rund ein Viertel ist direkt unter Linux installierbar. Für ungefähr die Hälfte der Applikationen ist eine gute Open Source Alternative verfügbar. Einzelne wenige Applikationen haben mit CrossOver funktioniert. Die restlichen Applikationen müssen als Citrix-Applikation genutzt werden, da keine der obigen Kategorien zutreffend ist bzw. funktioniert hat. Bei den meisten hat dieser letzte Ausweg auch funktioniert, aber zwei dieser Applikationen sind (noch) nicht auf Citrix verfügbar. Für diese wurde keine Lösung gefunden (**Fail** in der Tabelle in Abschnitt 4.2.6.1).

Das Zeitbudget für die Integration der Applikationen war von vornherein beschränkt, d.h. bei den Applikationen, die nicht funktioniert haben, wurde die Fehlersuche nach einer definierten Zeit abgebrochen (Kat 1: 4 Stunden, Kat2: 2 Stunden).

3.5.3 Fehlerklassen

Die Ergebnisse der Tests werden auf der Liste der Testfälle protokolliert. Für die Bewertung werden vier Bezeichnungen verwendet:

- "**Erfolgreich**": Die Applikation weist keinen erkennbaren Fehler auf
- "**Darstellungsmangel**": Die Applikation weist Mängel in der Darstellung, jedoch nicht in der Funktion oder der Datenverarbeitung auf. Diese Klasse wurde (vor allem bei den Piloten C/D/E) auch benutzt, um auf Mängel hinzuweisen, die zwar mit der Darstellung an sich nichts zu tun haben, aber als zu «harmlos» beurteilt wurden, als dass man sie schlechter bewertet wollte.
- "**Betriebseinschränkend**": Die Applikation enthält Mängel, die durch Umgehungslösungen durch die Anwendenden kompensiert werden können
- "**Betriebsverhindernd**": Die Applikation enthält Mängel, die sie für die praktische Arbeit unbrauchbar machen (Einschneidende funktionale Mängel oder fehlerhafte Datenverarbeitung)

3.6 Standardtests A/B

3.6.1 Crossover Applikationen

Crossover ist eine Software, die es ermöglicht, Windows-Programme auf Linux auszuführen. Da dies mit der Emulation der Windows-Systemaufrufe erfolgt und es keine Garantie für die Vollständigkeit der Emulation gibt, muss bei "Crossover-Applikationen" zusätzlich zur eigentlichen Funktion die Integration in den Desktop bzw. das Betriebssystem genauer geprüft werden. Folgende Testfälle sollten also zusätzlich definiert werden - sofern es jeweils einen entsprechenden Anwendungsfall dafür gibt:

- Desktop-Integration (copy&paste, drag&drop)
- Darstellung auf dem Bildschirm
- Unterstützung von Peripherie: Drucker, Lautsprecher/Mikrophon, optische Disks, USB-Geräte etc. die vom Applikationsverantwortlichen bereitgestellt wurden.
- Die Standard Ein- und Ausgabegeräte (Tastatur, Bildschirm, Maus) sind unterstützt.

3.6.1.1 Testfall 1: Desktop-Integration

- Copy & Paste: Von der Crossover-Applikation
  - In eine andere Crossover-Applikation
  - In eine native oder alternative Applikation
- Copy & Paste in die Crossover-Applikation
  - Von einer anderen Crossover-Applikation
  - Von einer nativen oder alternativen Applikation
- Verschieben von Dateien/Verzeichnissen aus dem/in den Windows-Explorer

3.6.1.2 Testfall 2: Darstellung

- Programm wird gestartet: Wird alles sauber dargestellt wie unter Windows: keine leeren oder verzerrten "Flecken", keine zu grossen/zu kleinen oder abgeschnittenen Texte, Texte sind gut lesbar?
- Fenster wird maximiert (full screen) und dann (an den Fensterrändern) verkleinert und wieder vergrössert: Ist die Darstellung immer noch einwandfrei?
- Können die Schriften vergrössert/verkleinert werden? Ist der Komfort ähnlich wie unter Windows? Sehen verkleinerte/vergrösserte Schriften gut aus (Anti-Aliasing)?

3.6.1.3 Testfall 3: Peripherie

- Kann die Peripherie wie unter Windows genutzt werden? (Für jede Peripherie gemäss Aufzählung oben in Abschnitt 3.6.1 einen Testfall definieren).

3.6.2 Citrix-Applikationen

Es gelten dieselben Feststellungen wie für Crossover-Applikationen. Im Gegensatz zu Crossover wird die Windows-Benutzendenschnittstelle nicht mit einer Emulation ins Betriebssystem eingebettet, sondern die Benutzendenschnittstelle der Applikation muss vom entfernten Host zum lokalen Desktop transportiert und so eingebettet werden.

Deshalb müssen dieselben Tests wie für Crossover durchgeführt werden (Testfall 1/2/3).

3.6.3 Web-Applikationen

Die ersten Standards für HTTP/HTML haben nur wenig Möglichkeiten geboten, interaktive Web-Applikationen umzusetzen (z.B. Formulare). Es gab deshalb auch relativ früh Erweiterungen, so genannte "plugins" (wie z.B. Flash), welche den Programmierenden mehr Freiheiten in der Umsetzung gaben. Der grosse Nachteil dieser plugins ist, dass sie abhängig vom Betriebssystem sind.

Web-Applikationen, die nur funktionieren, wenn ein bestimmtes plugin installiert ist, sind im engeren Sinn keine Web-Applikationen, sondern eher "Flash-Applikationen" oder "Java-Applikationen" etc. Meist sind sie auf ein Betriebssystem limitiert, manchmal sogar auf bestimmte Versionen des plugins. Mittlerweile wird die Unterstützung von plugins mehr und mehr aus den Browsern entfernt, nicht zuletzt weil diese Plugins immer wieder schwere Sicherheitslücken aufwiesen.

Mit der Einführung von neueren HTTP/HTML Standards (HTML 5, als "W3C Recommendation" seit Oktober 2014) wurde es möglich, vollständige Browser-Applikationen ohne Benutzung von plugins zu implementieren. Moderne Web-Applikationen verwenden keine plugins mehr.

3.6.3.1 Testfall 1: Plugin

- Wurde beim Starten der Applikation die Aktivierung eines Plugins verlangt? Welches?
- Start des Browsers im "safe mode" (d.h. alle plugins sind deaktiviert):
  - firefox –safe-mode
  - chromium-browser --incognito

3.6.3.2 Testfall 2: Browser-Unabhängigkeit

- Applikation sowohl in Chromium als auch in Firefox testen.

3.6.3.3 Testfall 3/4/5: wie oben Testfälle 1-3

- "Der Browser ist das Betriebssystem", also müssen diese Funktionen auch getestet werden.

3.7 Kostenvergleich

3.7.1 Lebenszyklen

Die Lebensdauer von Hardware hat sich in einem Bereich von 3 bis 6 Jahren eingependelt. Jedes Unternehmen ist gefordert, im Rahmen dieser Zyklen Ersatzbeschaffungen zu tätigen.

Die rasante Entwicklung der IT bringt es mit sich, dass die Erneuerungszyklen von Software immer kürzer werden. Aktuell werden die Softwarereleases in monatlichen Abständen aktualisiert. Wenn es sich dabei um eine Erweiterung eines bestehenden Produktes handelt, entstehen keine Migrations- und Ausbildungskosten, sondern höchstens ein überschaubarer Testaufwand.

Die Einführung eines OSS Produkts jedoch zieht den Aufbau der Plattform, die Migrations- und Ausbildungskosten nach sich. Diese Investitionen vor Ablauf eines Lebenszyklus zu machen, wäre dann sinnvoll, wenn sich sofort spürbare Einsparungen im Betrieb realisieren liessen, die in kurzer Zeit amortisiert wären. Das hat sich jedoch nicht als realistisch erwiesen.

Aus diesem Grund ist es sinnvoll, eine Umstellung auf OSS Produkte dann vorzunehmen, wenn durch eine notwendige Ersatzbeschaffung ohnehin eine Investition getätigt werden muss. Die Investition für den Aufbau einer neuen Plattform würde dann zu Teilen in eine OSS Plattform getätigt werden.

3.7.2 Mischbetrieb

Die Untersuchungen im Rahmen dieser Studie zeigen auf, dass eine vollständige Substitution von bestehenden Produkten durch OSS nicht realisierbar ist. Dies ist wie folgt begründet:

- Sehr fortgeschrittene Anwendenden (Power User) benutzen spezifische Funktionen (von z.B. Microsoft Word), zu welchen das OSS Alternativprodukt keine gleichwertigen Funktionen anbieten kann
- Viele Mitarbeitende sind auf den elektronischen Austausch von Dokumenten mit anderen Abteilungen oder externen Stellen angewiesen. Bei wechselseitiger Bearbeitung und damit wiederholter Konversion der Datenformate entstehen Formatierungsmängel, welche wiederholt manuell korrigiert werden müssen. Um diese Produktivitätsverluste zu vermeiden, empfiehlt es sich in diesen Fällen die Standard Produkte einzusetzen
- Fachapplikationen nutzen zum Datenaustausch oft Standard .xlsx oder .docx Dateien. Um eine aufwändige Anpassung von Schnittstellen zu vermeiden, ist es sinnvoller auch hier die Standardprodukte einzusetzen

Für diejenigen Mitarbeitenden, welche die Applikationen nicht extensiv nutzen und die nicht auf einen Datenaustausch mit anderen Stellen bzw. Fachapplikationen angewiesen sind, können OSS Produkte eingesetzt werden. Dies ist in der heutigen Situation nicht möglich. Um einen kostenoptimierten IT Betrieb zu erreichen, ist die Anzahl unterschiedlicher Applikationen möglichst tief zu halten. Der durch den Einsatz von OSS Produkten zwangsläufig erforderliche Mischbetrieb widerspricht diesem Grundsatz und führt zwangsläufig zu suboptimalen Betriebskosten.

3.7.3 Investitionen

Bei der Ermittlung des Investitionsbedarfs für die Einführung von OSS Produkten wurde versucht, die **Differenz** gegenüber der Einführung von den bisher eingesetzten Produkten abzuschätzen.

Einsparpotenzial:

- Entfall von hohen Lizenzinvestitionen von lizenzierten Produkten

Zusätzliche Investitionen:

- Aufbau von Know-how bei den Administratoren und dem Supportpersonal, da sie in der Regel mit den OSS Produkten nicht vertraut sind

- Zusätzlicher externer Support für den Aufbau der neuen Plattformen
- Aufwändigere Ausbildung der Anwendenden, da sie die Produkte nicht schon von Vorversionen oder vom privaten Einsatz her kennen
- Migration von Daten (Vorlagen, Dokumente) in auf die einzusetzenden OSS Produkte
- Anpassung von Schnittstellen der OSS Produkte z.B. zu den Fachapplikationen

3.7.4 Betriebskosten

Bei der Ermittlung der Betriebskosten von OSS Produkten wurde versucht, die **Differenz** gegenüber den bisher eingesetzten Produkten abzuschätzen.

Einsparpotenzial:

- Entfall von hohen wiederkehrenden Lizenzkosten der proprietären Produkte
- Entfall von hohen wiederkehrenden Wartungskosten der proprietären Produkte

Zusätzliche Betriebskosten:

- Zusätzlicher externer Support für den Betrieb der neuen Plattformen (Subscriptions)
- Betrieb und Support von zwei Plattformen, weil die Ablösung nicht vollständig möglich ist
- Betrieb von zusätzlichen OSS Plattformen führt zu Notwendigkeit von zusätzlichem Know-how Erhalt

3.7.5 Indikativer Kostenvergleich

Zum heutigen Zeitpunkt kann ein indikativer Kostenvergleich als Entscheidunterstützung erstellt werden. Dieser entspricht der Zielsetzung einer Potenzialanalyse, kann jedoch nicht alle Variablen und die Preisveränderungen bis zur konkreten Umsetzung genau beziffern. Bei einer konkreten Umsetzung sind zusätzlich folgende Faktoren kostenrelevant und müssen zu diesem Zeitpunkt im Detail erhoben werden:

- Die Marktsituation und die Preise werden sich bis zum konkreten Ersatz am Ende des Lebenszyklus eines Systems verändert haben
- Die Migrationskosten (Datenmigration / Schnittstellenanpassung) wurden abgeschätzt und dienen als Entscheidunterstützung. Vor dem Zeitpunkt der Umsetzung sind sie mit den derzeit gültigen Mengengerüsten und aktuellen Marktpreisen genau zu ermitteln
- Das Einsparpotenzial durch den Wegfall von Lizenzkosten beim Einsatz von OSS Produkten muss durch das Lizenzmodell gegeben sein, sonst kann die Einsparung nicht realisiert werden.

Für jedes Pilotprojekt wurde eine Kostentabelle mit den Investitonen und den Betriebskosten erstellt, welche die Differenz gegenüber der heutigen Situation darstellt.

4 Pilotprojekt A: Basis Client

4.1 Anforderungsdefinition

Um einen OSS-Client im Umfang des bestehenden Windows-Clients bereitzustellen, müssen folgende Fragestellungen gelöst werden:

Funktionalität: Wie wird sichergestellt, dass alle ihre Arbeit möglichst effektiv mit dem Client erledigen können?

- Welche Personen benutzen welche Applikationen und Daten? **Benutzendenkonzept** mit Personen (Authentisierung) und Gruppen (Autorisierung).
- Erfüllt die installierte Software die Bedürfnisse der Anwendenden? Pflege eines **Applikations-Inventars**.

Betriebliche Anforderungen: Wie wird sichergestellt, dass die Clients funktionieren und sicher sind?

- Wie wird eine neue Hardware ab Werk so bereitgestellt, dass die Angestellten sofort damit arbeiten können? Automatisierter **Rollout**.
- Regelmässige Aktualisierung von Betriebssystem, Applikationen und Konfigurationen.
- Monitoring und Remote-Support.
- Wie wird sichergestellt, dass Daten nicht in die falschen Hände geraten: Benutzendenkonzept, Verschlüsselung, …
- Die Stadt Bern betreibt über 2200 Clients, davon sind 65 % Thin Clients. Ein **Rollout** muss so einfach wie möglich sein.
- Die Stadt Bern hat ein Microsoft Active Directory als Implementation des **Benutzendenkonzepts**, ein Client muss sich darin integrieren.

Das **Applikations-Inventar** der Stadt Bern umfasst total ca. 230 Applikationen. Davon sind 30 KAT1 und 17 KAT2 Applikationen. Ein Client muss (für Pilot A) die Funktionalität der KAT1 und KAT2 Applikationen abdecken. KAT1 Software wird auf jedem Client, KAT2 Software auf "den meisten“ Clients installiert.

Die Stadt Bern hat einen Katalog mit **Sicherheitsanforderungen** an einen Client. Dieser orientiert sich an gängigen Standards wie dem IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik Deutschland) und muss eingehalten werden.

4.2 Umsetzung

4.2.1 Lösungsansatz

Die Umsetzung von Pilotprojekt A besteht aus folgenden Phasen. Die ersten zwei sind vollautomatisiert, der letzte Schritt wird im Rahmen des Pilotprojekts manuell durchgeführt:

1. Rollout des Betriebssystems: Auf einem "leeren“ Rechner wird das Betriebssystem installiert.
2. Auf dem Betriebssystem werden die Applikationen installiert (und bei Bedarf aktualisiert).
3. Beitritt zur Windows-Domäne (AD-Join).

4.2.2 Rollout Betriebssystem Basis Client

Als Basis-Distribution für den Client wurde openSUSE gewählt, weil zum Zeitpunkt des Entscheids SUSE die einzige Plattform war, auf der in Zukunft SAP Datenbanken betrieben werden konnten und es sinnvoll ist, die Anzahl verschiedener Distributionen in einer Organisation möglichst tief zu halten.

Beim automatisierten Rollout bootet die Hardware (oder die VM) vom Netz, partitioniert die Harddisk und installiert das Betriebssystem nach den zentralen Vorgaben ohne dass auf der Hardware selbst schon irgendwelche Konfigurationen/Installationen vorgenommen wurden.

4.2.3 Exkurs: Vergleich zentrale Steuerung Clients

Werden in einem Netzwerk viele identische Clients benötigt, aber die Benutzenden sollen eigene Rechte, Konfigurationen und Daten haben, braucht es einen technischen Unterbau für die Umsetzung dieser Anforderung. Für Windows-Clients sind folgende Mechanismen zentral:

- Logon-Script macht abhängig vom Benutzendennamen (und seinen Gruppenmitgliedschaften) verschiedene Netzwerklaufwerke mit verschiedenen Zugriffsrechten in der Benutzendensession zugänglich. Wichtigstes Laufwerk ist das Heimlaufwerk.
- Mit sogenannten GPOs können vom Server her Registry-Einstellungen auf dem Client gesetzt werden. So kann zum Beispiel gezielt eine bestimmte Funktionalität in einem Programm abgeschaltet werden.

Linux-Clients haben keine Registry. Unter Linux ist «alles» eine Datei. Applikationen beziehen Ihre Einstellungen aus Konfigurationsdateien. Die meisten Applikationen konsultieren zuerst eine globale Konfigurationsdatei (diese kann der Benutzende nicht verändern) und dann eine lokale (aus dem Heimverzeichnis des Benutzenden). Um Client-Applikationen zentral zu konfigurieren, müssen also die Konfigurationsdateien verändert werden. Dies ergibt für Linux die folgenden Mechanismen:

- Das Einhängen der Netzwerklaufwerke läuft bei Linux ähnlich wie bei Windows. Linux kennt keine Laufwerk-Buchstaben, externe Verzeichnisse werden in den Datei-Baum eingehängt. Das Heimverzeichnis wird unter Linux normalerweise unter /home eingehängt (z.B. /home/user), weitere Netzwerklaufwerke für die Benutzenden-Sitzung direkt darin (also /home/user/BernProjekte).
- Einstellungen an Konfigurationsdateien werden im hier vorgeschlagenen Setup durch die Ansible-Scripts (siehe weiter unten in 4.2.5.1) sichergestellt.

4.2.4 Client Einstellungen

Die meisten Anforderungen für diese Einstellungen stammen aus den Client-Security-Vorgaben der ID der Stadt Bern.

4.2.4.1 Screenlock

Ein Screenlock ist bei der GNOME Oberfläche dabei. Die Zeit, nach welcher der Screenlock automatisch aktiviert wird, wurde auf 5 Minuten festgelegt.

4.2.4.2 Privilege Escalation

Der User "root" hat ein Passwort, damit notfalls ein Login ohne Active Directory/LDAP möglich ist. Dieses zu deaktivieren ist möglich, setzt aber voraus, dass den Linux Administratoren sudo-Rechte gegeben wird. Im laufenden Betrieb sollte es keinem normalen User möglich sein, root-Rechte zu erlangen.

4.2.4.3 Full Disk Encryption

Die Anforderungen der ID der Stadt Bern an ein Client Gerät ist einerseits, dass die gesamte Harddisk verschlüsselt ist und andererseits, dass jedes Gerät von jeder berechtigten Person genutzt werden kann.

Dies ist mit einem aktuellen Linux Betriebssystem nicht möglich. Das erprobte Tool unter Linux für Full Disk Encryption ist LUKS. Dabei wird vor dem eigentlichen Start des Betriebssystems ein Passwort abgefragt. LUKS kann aber höchstens 8 verschiedene Passwörter verwalten.

Man kann sich eine Lösung vorstellen, wo jeweils die Passwörter der letzten sieben Benutzenden (ein Slot sollte immer für ein Passwort reserviert sein, welches die Administratoren der ID der Stadt Bern wissen) automatisch eingetragen werden. Eine Abklärung, ob so eine Lösung für das Schlüsselmanagement für die Stadt Bern genügen würde, sprengt den Rahmen einer Potenzialanalyse.

4.2.4.4 Firewall

Auf den Clients läuft eine Firewall, welche mit iptables/netfilter und dem Frontend von YaST verwaltet wird. Grundsätzlich sind alle ausgehenden Verbindungen erlaubt. Eingehend ist nur SSH erlaubt, da dies für die Remote Administration und für Support gebraucht wird.

4.2.4.5 Password Security

Die Clients werden mit Hilfe von sssd am zentralen Active Directory der Stadt Bern authorisiert. Durch sssd ist es möglich, dass sich die User mit ihrem Active Directory Login am Client einloggen und dass andere Passwörter (zum Beispiel lokale) ungültig sind. Nach einem erfolgreichen Login stellt der sssd auch sicher, dass sich für eine gewisse Zeit (normalerweise 1 Monat) derselbe User wieder anmelden kann, auch wenn das Active Directory nicht erreichbar ist (Laptops).

Ein Wechsel des Passworts ist am Client ebenfalls möglich, allerdings nur wenn es eine aktive Verbindung zum Active Directory gibt. Dies entspricht dem Verhalten unter Windows. Wie bisher wird durch das AD sichergestellt, dass die Benutzenden genügend komplexe Passwörter (Länge, Sonderzeichen, …) verwenden.

4.2.4.6 Updates und Security Patches

Die Installation von Updates und Patches ist Teil des automatischen Rollouts, im Wesentlichen wird der dritte Schritt („Ansible“, siehe 4.2.5.1) regelmässig wiederholt.

Dabei werden auch alle Software-Pakete aktualisiert, die in neueren Versionen in den Repositories vorliegen. Für den Pilotbetrieb wurden der Einfachheit halber die öffentlichen OpenSUSE-Repositories als Quelle konfiguriert. In einer produktiven Installation würde ein eigener Klon des Repositories als Quelle benutzt. Aktualisierte Pakete würden dort erst nach einer internen Freigabe bereitgestellt. Auf eine Implementierung wurde verzichtet, da es für den Client funktionell irrelevant ist, welches Repository als Quelle konfiguriert ist.

4.2.4.7 Malware

Auf den Systemen läuft ein TrendMicro AntiVirus, welches bei der Stadt Bern auch Serverseitig eingesetzt wird. Dieses bietet die Möglichkeit, die Berichte an einen zentralen Server zu schicken und schützt vor gängiger Malware. Die Pilot-Installation umfasst lediglich die Linux-Standard-Konfiguration mit regelmässigen Disk-Scans ohne „Live“-Überpüfung (z.B. beim Speichern einer Datei). Gemäss Hersteller-Informationen kann eine Live-Überprüfung eingerichtet werden. Das dazu notwendige Kernel-Modul kann über DKMS integriert werden.

4.2.4.8 E-Mail Client

Der E-Mail Client, welcher auf die Groupware Lösung zugeschnitten ist, wird durch das Pilotprojekt C evaluiert. Aus diesem Grunde wird das Thema in diesem Teilprojekt nicht genauer behandelt.

4.2.4.9 Integration Stadt Bern Netzwerk

Die Clients sind am Active Directory angehängt, dies bedeutet, dass sich die User mit ihren Active Directory Passwörtern einloggen können. Welcher User welche Shares bekommt, wird durch dessen Gruppenzugehörigkeit und eine Konfigurationsdatei (welche durch Ansible gemanaged wird) gesteuert. Dies ist unabhängig davon, welche Rechte ein User auf den Fileservern hat.

Auf den Clients ist der Follow2Print Drucker eingerichtet und das Hintergrundbild angepasst.

Die Clients werden nur per Ethernet ins Netzwerk integriert. WiFi ist zwar installiert, aber lediglich bereit für eine manuelle Konfiguration eines beliebigen „Gäste-WLANs“.

4.2.4.10 Personalisierung

Die Spracheinstellungen sind auf Schweizerdeutsch gesetzt und eine Liste von Schriftarten wird von Linux selbst direkt mitgebracht, es sind aber keine zusätzlichen speziellen Schriftarten installiert, weil hierzu keine Anforderung definiert wurde.

4.2.4.11 Browser

Da beim aktuellen Windows Client der Browser Google Chrome normalerweise zum Einsatz kommt, wird beim Linux Client der Browser Chromium verwendet, welcher ein OpenSource Klon des Google Chrome ist.

Google Chrome wird beim aktuellen Client im Incognito Modus gestartet, weil diese Einstellung aus Sicherheitssicht als sehr gut angeschaut wird. Diese Einstellung ist so bei Chromium übernommen worden, damit wir hier keinen Verlust an Sicherheit haben. Bookmarks sind keine Importiert, können aber wie beim Google Chrome durch den Benutzenden verwaltet werden.

Zentrale Browser-Konfigurationen, welche heute per GPO verteilt werden, können analog in die „Ansible“-Konfiguration (siehe 4.2.5.1) der Clients aufgenommen werden. Es ist eine Frage jeder einzelnen Applikation, wie gut sie unter Linux zentral konfiguriert werden kann. Ob Chromium (oder Chrome) unter Linux gleich gut wie unter Windows mit GPO gesteuert werden kann, wurde nicht analysiert.

4.2.4.12 Office

Als Ersatz von Microsoft Office kommt LibreOffice zum Einsatz. LibreOffice ist für Benutzende von Microsoft Office zwar etwas ungewohnt, aber über weite Strecken eine gute Alternative. Microsoft Office-Dokumente können importiert und exportiert werden. Wie die Tests zeigten, ist ein Ersatz doch sehr schwierig[1].

Es wäre (mit der neusten Version von CrossOver) auch eine Installation von Microsoft Office 2016 möglich. Diese Version CrossOver war leider erst gegen Ende der Implementationsphase erhältlich, es fanden damit keine Tests mehr statt. Auch würde eine solche Implementation eines der Ziele dieser Analyse – Reduktion der Microsoft-Lizenzen – direkt ad absurdum führen.

4.2.4.13 Applikations-Pakete

Damit eine Software auf einem Linux-System installiert werden kann, muss sie in einem sogenannten Paket bereitgestellt werden. Software-Pakete werden in Repositories bereitgehalten. Die gesamte Software (auch das Betriebssystem) liegt in Paket-Format vor, bei SUSE als RPM-Paket. Dies erlaubt eine einfache, einheitliche Verwaltung von Software-Versionen, -Updates etc. Für die Variante "native“ oder "Alternative“ werden die RPM-Pakete meistens vom Hersteller und/oder von der Distribution zur Verfügung gestellt. Diese müssen lediglich ins Paket-Repository kopiert werden und in die Ansible-Scripts integriert werden.

Für "Crossover“ müssen die RPM-Pakete selber erstellt werden, siehe dazu den nächsten Abschnitt.

Für die Variante "Citrix-Applikation“ ist nichts zu tun: Die Applikation wird via Browser gestartet und die bestehende Berechtigungslogik in Citrix greift automatisch. Eine Integration ins Start-Menü wurde nach ersten Abklärungen gemäss der Feature-Matrix[2] als nicht möglich eingeschätzt.

[1] Siehe dazu zum Beispiel TFA34 (4.3.2.7)

[2] https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf

4.2.4.14 Crossover

Crossover ist ein Produkt der Firma Codeweavers[3]. Es handelt sich um eine professionalisierte Version der Open Source Software WINE[4]. Mit WINE können Windows-Applikationen auf Linux laufen. WINE kann man sich als "Vermittler-Schicht“ zwischen einer Windows-Applikation und dem Linux-Unterbau vorstellen: WINE täuscht der Applikation vor, auf einem Windows-System zu laufen, indem es die windowsspezifischen Systemaufrufe in entsprechende Aufrufe für Linux umwandelt. Dieser Ansatz ist in der Industrie durchaus üblich, zum Beispiel bietet Microsoft ihr Datenbank-Produkt MSSQL mit einer ähnlichen Zwischenschicht kommerziell auf Linux an.

Leider gibt es keine vollständige (und öffentlich verfügbare) Liste aller Windows-Systemaufrufe. Und selbst wenn es sie gäbe, würde sie mit jeder Windows-Version wachsen. Damit muss CrossOver/WINE immer wieder an die neusten Windows-Versionen angepasst werden und hinkt Windows selbst immer nach.

Crossover ermöglicht es, eine oder mehrere Applikationen zusammen mit WINE in ein RPM-Paket zu verpacken. Trotz technischer Unterstützung ist dies ein Prozess, der relativ viel Engineering-Aufwand benötigt (siehe Beschreibung im nächsten Kapitel) und es gibt keine Garantie, dass die Applikation am Schluss auch funktioniert.

Es kann davon ausgegangen werden, dass kaum ein Software-Hersteller Support für die Ausführung seiner Windows-Applikation unter Crossover bietet. Trotzdem wurde diese Variante getestet, um eine Aussage über die technische Machbarkeit machen zu können.

4.2.4.14.1 Vom Windows-Programm zum RPM

Crossover verwendet für die Erzeugung eines RPM-Pakets sogenannte "Bottles". Eine Bottle ist eine separate, lokale Installation von WINE auf einem Entwicklungsrechner. In eine Bottle können eine oder mehrere Applikationen installiert werden, aber es gibt immer ein RPM-Paket pro Bottle.

Auf dem Entwicklungsrechner wird also pro zu erzeugendes RPM-Paket eine Bottle erstellt, die Applikation in diese Bottle installiert und dort provisorisch getestet. Funktioniert alles, wird daraus das RPM-Paket erstellt, welches dann später automatisch auf den produktiven Clients installiert werden kann. Die beiden nächsten Abschnitte beschreiben dies etwas detaillierter.

4.2.4.14.2 Einrichten einer Bottle

- Bottle mit ‘Add’ hinzufügen.
- Als Name wird der Name der darin zu installierender Software gewählt z.B. Notepad++
- Unter dem Typ wird angegeben, welche Windows Version verwendet werden soll (ähnlich wie der Kompatibilitätsmodus unter Windows 7+). Oft lassen sich die Applikationen besser unter Windows mit 32bit Architektur installieren als mit 64bit.

4.2.4.14.3 Installieren der Windows Software in die Bottle

Die Applikation wird über den Button ‘Install Windows Software...’ installiert.

Select Application

Im Suchfeld wird nach der zu installierenden Software gesucht. Bei einem Treffer sind sämtliche notwendigen Einstellungen für die Bottle (Abhängigkeiten, Parametrisierung) definiert und die Applikation kann dann in die Bottle installiert werden.

[3] https://www.codeweavers.com/products/crossover-linux

[4] https://www.winehq.org/

Gibt es für die gesuchte Software noch keinen Eintrag, dann muss "Unlisted application" ausgewählt werden. In diesem Fall müssen alle Windows Einstellungen und Abhängigkeiten im Schritt "Install&Finish" selber eingerichtet bzw. nachinstalliert werden.

Select Installer

Über den Button "Choose Installer File..." wird das .exe oder .msi File der zu installierenden Applikation gesucht und dann ausgewählt. Steht die Applikation als separates Medium (USB Stick, optische Disk, ISO-Image) zur Verfügung, dann kann der Inhalt des Mediums zuerst in ein lokales Verzeichnis kopiert werden und dann das entsprechende Verzeichnis über den Button "Choose Installer Folder..." ausgewählt werden.

Select Bottle

Jetzt wird die Bottle aus dem vorderen Schritt ausgewählt.

Install & Finish

Über den Button "**Advanced Options**" werden noch weitere Abhängigkeiten wie zum Beispiel ".NET Framework" oder "Visual X Runtime" mit installiert. Dies ist dann einfach, wenn diese Abhängigkeiten bekannt sind. Meistens sind diese aber nicht dokumentiert (weil sie unter Windows "selbstverständlich" sind) und müssen mehr oder weniger experimentell ermittelt werden. Dieser Schritt macht den Aufwand (und das Risiko) aus. Mit dem "**Add**" Button können alle verfügbaren Pakete angezeigt und bei Bedarf hinzugefügt werden. Unter den "**Logging Optionen**" kann man das Logging während der Installation (auf dem Entwicklungsrechner) anpassen.

Durch Klicken auf "**Install**" wird der Windows Installer gestartet und die Installationsroutine der .exe oder .msi Datei gestartet.

4.2.5 Konfiguration Infrastruktur

Das vorliegende Kapitel beschreibt kurz die Infrastruktur für den automatischen Rollout eines Clients (Installation Betriebssystem und Applikationen):

Von der Stadt Bern mitbenutzt:

- DHCP Server. Anpassung der Konfiguration für PXE-Boot
- Administrations-Zugang vmware
- Zwei virtuelle Clients

Bei der Stadt Bern neu eingerichtet:

- virtueller Server mit Foreman
- Package Repository für die “eigenen” Pakete

Bei Adfinis SyGroup mitbenutzt:

- Git für die Ansible Scripts

4.2.5.1 Installation Basis-Client

Die automatische Installation ist mit Foreman umgesetzt. Via Web Frontend muss ein neuer Client zunächst erfasst werden. Im Wesentlichen ist das ein Hostname, eine MAC-Adresse und das root Passwort. (Der Import von grösseren Mengen müsste via API programmiert werden).

Sobald ein Client in Foreman erfasst ist und dann per PXE Boot startet, erhält er von Foreman die nötigen Instruktionen für die Basis-Installation und führt sie dann aus. Die Basis-Installation ist abgeschlossen, wenn der Client nach einem reboot soweit konfiguriert ist, dass er sich beim Konfigurationsmanagement-system einmal täglich Aktualisierungen abholt. Die Aktualisierungen gehen vom Client aus (pull).

Beim initialen Setup eines Clients muss aktuell abgewartet werden, bis der Client den ersten Konfigurationslauf durchführt, erst dann werden alle Applikationen installiert. Dies könnte aber mit relativ einfachen Mitteln automatisch beim ersten Boot eingebaut werden. Ein Konfigurationslauf kann manuell vorzeitig angestossen werden, indem "/etc/cron.daily/ansible-pull“ (als root) gestartet wird. Das root Passwort wurde von Foreman gesetzt.

Die Konfigurationen sind in Ansible implementiert und werden auf einem git Server verwaltet. Ansible-Konfigurationen sind idempotent, d.h. es gibt keinen Unterschied in der Konfiguration nach erstmaliger Installation und nach Aktualisierung. Ansible-Scripts können Systemeinstellungen anpassen (zum Beispiel das Timeout des Screen Locks), Software installieren (oder deinstallieren) etc. Durch das tägliche Durchführen eines Konfigurationslaufs ist sichergestellt, dass alle Clients auf dem aktuellsten Stand sind.

Schliesslich ist ein Join des Clients ins Active Directory notwendig – dies braucht einen AD-User mit Domain-Admin-Rechten. Gemeinsam mit der Stadt Bern wurde entschieden, den Client ins produktive Netz zu stellen, deshalb braucht es auch einen produktiven AD-User. Aus Datenschutzgründen wurde dieses Passwort aber nie an Mitarbeiter von Adfinis SyGroup AG abgegeben, dieser Schritt muss also durch einen Mitarbeiter der Stadt Bern durchgeführt werden (Bei anderen Kunden wurde ein Passwort für den Domain-Join im Foreman hinterlegt): Login als root, ausführen von "adjoin“.

4.2.6 Funktionstest

Für Applikationen, welche mit Crossover installiert wurden, wurde bereits während der Paketierung ein kleiner Funktionstest durchgeführt: Da zum Zeitpunkt dieser Arbeiten die detaillierten Anforderungen noch nicht festgelegt waren, beschränkte sich dies in der Regel darauf, zu kontrollieren, ob die Applikation überhaupt startet.

4.2.6.1 Ergebnis Installationstest Kat 1 / Kat 2

Wie in Abschnitt 3.5.2 dargelegt, wurde jeweils die "bestmögliche" Umsetzung gewählt. Die problematischen Fälle sind **fett** markiert:

- **Fail** bedeutet, dass kein Weg gefunden wurde, die Applikation (oder etwas ähnliches) unter Linux zum Laufen zu bringen. Achtung: Das ist kein abschliessendes Urteil. Es ist durchaus möglich, dass mit mehr Aufwand oder einer neueren Version "Crossover" doch noch ein Erfolg möglich wäre.
- **Citrix-App** bedeutet, dass lediglich die von der Stadt Bern virtualisierte Variante zum Laufen gebracht werden konnte. Technisch funktioniert das zwar einwandfrei, aber es können kaum Lizenzen eingespart werden (da für die Ausführung immer noch eine Windows-Lizenz notwendig ist). Auch ist eine offline-Nutzung nicht mehr möglich.

Die untenstehende Tabelle zeigt die Ergebnisse für die Umsetzung pro Applikation, zuerst werden die Kat1-, dann die Kat2-Applikation aufgelistet.

Applikation	Lösung	OSS Alternative	Notizen
K1 TFA01 Acro Software CutePDF Writer	Alternative	cups-pdf	
K1 TFA04 Adobe Flash Player	Nativ		
K1 TFA05 Adobe PDF iFilter	**Fail**		Setzt auf Windows Search auf
K1 TFA07 Adobe Reader DC	Alternative	evince	
K1 TFA12 Citrix Receiver	Nativ		

Applikation	Lösung	OSS Alternative	Notizen
K1 TFA13 E3	**Citrix App**		Startet (bei CrossOver) nach der Installation nicht, steht aber virtualisiert zur Verfügung.
K1 TFA16 Freemind	Nativ		
K1 TFA18 Google Chrome	Alternative	chromium	
K1 TFA19 Greenshot	Alternative	gnome-screenshot	
K1 TFA21 Igor Pavlov 7-Zip	Nativ		
K1 TFA23 K-Lite Codec Pack Mega	Alternative		Unter Linux werden keine zusätzlichen Codecs gebraucht
K1 TFA24 Microsoft Edge Browser	Alternative	Firefox	
K1 TFA25 Microsoft Internet Explorer	Alternative	Firefox	
K1 TFA26-34Microsoft Office Professional Plus 2016	Alternative	LibreOffice	
K1 TFA40 Ontrex Nexthink Collector	~~Alternative~~ **Fail**	~~VNC~~	Hat sich beim Review als falsche Alternative heraugestellt.
K1 TFA41 Oracle Java	Alternative	OpenJDK 1.8	
K1 TFA42 SAP Logon PAD	**Citrix App**		Konnte (unter Crossover) nicht paketiert werden, steht aber virtualisiert zur Verfügung.
K1 TFA43 Stadt Bern In4mer Client	**Fail**		Startet (bei CrossOver) nach der Installation nicht.
K1 TFA44 Tools4Ever UMRA Automation	**Citrix App**		Startet (bei CrossOver) nach der Installation nicht, steht aber virtualisiert zur Verfügung.
K1 TFA45 TrendMicro OfficeScan Agent XG	Nativ		Für Live-Scans muss ein Kernel-Modul mit DKMS integriert werden.
K1 TFA46 VLC Media Player	Nativ		
K1 TFA47 Zope External Editor	Nativ		
K2 TFA02 Adobe Acrobat Pro DC	Alternative	Scribus	
K2 TFA03 Adobe Creative Cloud Suite	Alternative	Inkscape, Blender	
K2 TFA06 Adobe Premiere Elements	Alternative	kdenlive	

Applikation	Lösung	OSS Alternative	Notizen
K2 TFA08 Avanti SSO Agent 2.0.0.1	**Citrix App**		Steht virtualisiert zur Verfügung.
K2 TFA09 Avery Design & Print	CrossOver		
K2 TFA10 Banana Buchhaltung	CrossOver		
K2 TFA11 Brother P-Touch Editor	**Citrix App**		Startet (bei CrossOver) nach der Installation nicht, steht aber virtualisiert zur Verfügung
K2 TFA14 EIDEN Schichtplaner	CrossOver		
K2 TFA15 FileZilla	Nativ		
K2 TFA17 Gimp	Nativ		
K2 TFA20 IDM UltraEdit	Nativ		
K2 TFA22 IrfanView	Alternative	Shotwell	
K2 TFA35 Microsoft Project Standard	**Citrix App**		Startet (bei CrossOver) nach der Installation nicht, steht aber virtualisiert zur Verfügung
K2 TFA36 Microsoft Visio Standard	Alternative	LibreOffice Draw	
K2 TFA37 Mirko SuperMailer	**Citrix App**		Startet (bei CrossOver) nach der Installation nicht, steht aber virtualisiert zur Verfügung
K2 TFA38 Notepad++	Alternative	Geany	
K2 TFA39 Nuance OmniPage Ultimate	**Fail**		Konnte (unter Crossover) nicht paketiert werden

Zu den beiden Applikationen "TFA43 Stadt Bern In4mer Client" und "TFA39 Nuance OmniPage Ultimate" noch je eine Bemerkung:

Der **In4mer Client** ist eine (relativ einfache) Eigenentwicklung der Stadt Bern, diese liesse sich mit vertretbarem Aufwand auch für Linux entwickeln.

OmniPage hingegen ist die führende Applikation für die Digitalisierung von ausgedruckten Dokumenten: Zentral ist die integrierte OCR, welche nicht nur den Text, sondern auch das Layout (z.B. einspaltig vs mehrspaltig) erkennen kann. Zwar erreicht auch OmniPage keine 100% Erkennungsrate, ist aber den verfügbaren Open Source Lösungen bei weitem überlegen. Der Hersteller bietet für Linux ein "SDK" an, das heisst die Kernkomponente OCR könnte auch in Linux-Lösungen eingebaut werden, aber es gibt keine fixfertige Desktop-Applikation.

4.2.7 Security

4.2.7.1 Externes Audit des OSS Clients

Im Rahmen des Audits wurde ein Client mit einem installierten openSUSE Leap 42.3 Linux auf die Sicherheit überprüft. Obwohl der getestete Client nur mässig gehärtet ist und mehrheitlich der Standardkonfiguration entspricht, stellt sich die Frage, ob es möglich ist einen Linux Client mit derselben Sicherheit wie der aktuelle Windows10 Client der Stadt Bern bereitzustellen.

Aus sicherheitstechnischer Sicht spricht gemäss Oneconsult nichts gegen einen Client mit einem Linux Betriebssystem. Ein Linux kann mindestens genauso gehärtet werden, damit es den Sicherheitsanforderungen des aktuellen Windows 10 Clients der Stadt Bern entspricht. Dazu muss im Vergleich zum getesteten Linux Client jedoch noch in einigen Bereichen nachgebessert werden.

Nachfolgend eine Zusammenfassung der Bereiche, welche noch Verbesserungspotenzial haben:

- Entfernen oder härten von (unnötigen) Diensten
- Härtung der Netzwerkkonfiguration
- Härtung des Dateisystems
- Updatemanagement
- Logging und Monitoring
- BIOS/UEFI und Bootvorgang

Installieren und konfigurieren von sicherheitsrelevanten Programmen oder Technologien wie:

1. Antivirus
2. Hostbasierte Firewall
3. Mandatory Access Control (MAC)

Bei der Implementierung von weiteren Programmen oder Funktionalitäten empfiehlt Oneconsult, diese soweit möglich zu härten und dabei auf bewährte «Hardening Guides» von CIS, NIST, BSI oder ähnlichen Organisationen zurückzugreifen.

4.2.7.2 Automatisierung des Domänenbeitritts

Wie oben in 4.2.5.1 beschrieben, muss im aktuellen Pilotbetrieb der Domänen-Beitritt manuell durch Mitarbeitende der ID der Stadt Bern durchgeführt werden. Dies könnte einfach automatisiert werden, wenn das Domänen-Passwort auf "Foreman" hinterlegt würde. Allerdings verleiht das Domänen-Passwort dem Eigentümer viel Macht. Es muss also sorgfältig zwischen Bequemlichkeit und Sicherheit abgewogen werden. Da bei Sicherheit die Details entscheidend sind, kann im Rahmen des Pilotprojekts keine Antwort gegeben werden, wie dies konkret umgesetzt werden sollte. Es ist aber davon auszugehen, dass eine Lösung gefunden werden kann, schliesslich existiert bereits eine akzeptable Lösung für die jetzige Windows-Infrastruktur.

4.2.7.3 Single Sign On

Die Stadt Bern benutzt unter Single Sign On Lösungen von anderen Verwaltungen für den Zugriff auf deren Web-Applikationen (Kanton Bern, Bund). Diese Lösungen brauchen zum Teil spezielle Hardware und müssen deshalb auch direkt unter Linux implementiert werden, eine als Fallback implementierte Citrix-Applikation reicht nicht. Diese Abhängigkeiten waren im Applikationsinventar leider nicht ersichtlich und wurden deshalb erst während den Tests entdeckt. Die betroffenen Applikationen haben deshalb den Test nicht bestanden. Bei einer allfälligen Migration auf Linux wäre es deshalb unabdingbar, dass sämtliche Abhängigkeiten zwischen den Applikationen bekannt sind.

4.3 Testdurchführung

4.3.1 Grundsätzliches

Die Applikationen KAT1 sind auf jedem Client verfügbar und gleichzeitig die meistgenutzten Anwendungen. Vollständiges Funktionieren dieser Basis Applikationen bzw. deren OSS Alternativen ist zwingend betriebsnotwendig.

Die Applikationen KAT2 werden verbreitet genutzt und decken ergänzende Benutzendenanforderungen für die tägliche Arbeit ab.

Abhängig von der Installationsart werden die Applikationen mit unterschiedlichen Methoden getestet. Es wird zwischen "Nativ", "Alternative", "Crossover", "Citrix-App" und "WEB Applikation" unterschieden.

4.3.2 Testfälle/Ergebnisse pro Applikation

Die Bewertungen wurden von den Testpersonen vergeben. Ob die Stadt Bern ihre Arbeit (zum grössten Teil) auch auf einen Open Source Desktop erledigen können, hängt von der Tauglichkeit der am meisten benutzten Applikationen ab. Die meisten Geschaftsvorfälle produzieren letzlich ein Dokument, aus diesem Grund wurde hier der Fokus auf das Testing der Office-Alternative LibreOffice gelegt. Dazu gehört im weiteren Sinne auch noch der «Werkzeugkasten» für .pdf-Dateien.

4.3.2.1 TFA01 / 02 / 07 CutePDF Writer, Acrobat Pro DC, Adobe Reader DC

Obwohl PDF ein offengelegtes, weit verbreitetes, als PDF/A sogar als geeignet für die Langzeit-archivierung gilt, unterstützen die OSS-Programme in der Regel nicht alle Funktionalitäten der Adobe-Programme. Auch sind die Funktionalitäten unter Umständen anders auf die verschiedenen OSS Programme verteilt als auf die jetzt verwendeten Programme.

Die Testfälle wurden interaktiv mit dem Applikationsverantwortlichen für die meisten der betroffenen Programme aufgestellt und gleich durchgeführt.

Zusammenfassend lässt sich sagen, dass der Grossteil der notwendigen Bearbeitungen von .pdf-Dateien auch mit OSS-Produkten gelingen würde. Leider gibt es auch hier einige Anwendungsfälle, die mit OSS-Tools nicht oder nur über Umwege gelingen. Und gerade diese wären für den professionellen Einsatz in der Druckvorstufe notwendig.

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA01-001	**Print to PDF** (aus jeder Applikation, die drucken kann, ein einfaches PDF erstellen) cutepdf vs linux pdf print Drucken einer beliebigen Webseite auf CUPS-PDF aus Firefox CUPS-PDF speichert die Daten unter /var/spool/cups/idenis (wenn der Benutzende "idenis" ist). Das ist für Benutzenden unschön (und nur das ist mit «Darstellungsmangel» gemeint). Könnte aber (mit einem symlink) relativ einfach gelöst werden.	Darstellungsmangel
TFA02-001	**PDF editieren** (nur jeweils auf einer Seite, kann aber Zeilen hinzufügen) Test mit libreoffice und «Arbeitsblatt.pdf» Der PDF-Import in LibreOffice gelingt nur in eine Libre-Office "Drawing"-Datei (.odg) (also als Bild). Die Layout-Erkennung (Tabellen) ist in proDC besser. Würde als Workaround gemäss AV aber gerade noch genügen, aber letztlich kann nur ein Bild (und kein Textdokument) editiert werden.	Betriebseinschränkend
TFA02-002	Konversion zu docx geht nicht, siehe TFA02-001	Betriebsverhindernd
TFA02-003	Konversion zu xlsx geht nicht, siehe TFA02-001	Betriebsverhindernd
TFA02-004	Formular generieren/definieren	Betriebseinschränkend

	libreoffice: Erzeugen eines einfachen, einseitigen Testformulars mit mind. zwei Eingabefeldern, Test mit «PDFFormular.odt/.pdf» Die Erzeugung eines PDF-Formulars gelingt in libreoffice, aber man kann nicht wie in pro dc in einem Tool bleiben um auch gleich zu testen. Problemstellung lässt sich also lösen, ist aber mühsamer.	
TFA02-005	indesign / illustrator / photoshop benutzen **distiller (aus pro dc)** für die Generierung PDFs für die Druckvorstufe (zB PDF/X-3) **scribus** output prüfen (mit «ScribusTest.sla/.pdf »). Resultat muss auf CLIMB Rechner in pro dc importiert/analysiert werden. Randmarken und Farbbänder können gemacht werden. Leider schneidet scribus beim Output Formen, die über den Rand gehen, bündig zu den Randmarken ab. Diese sollte weitergehen, ansonsten kann es bei kleinen Abweichungen beim Schneiden des Papiers weisse Ränder geben. Weiter berichtet der AV, dass er bei früheren Versuchen recht zufrieden war, wenn man eine Datei direkt in Scribus erstellt. Aber der Import von indesign Files gelingt nur zu ca 60%.	Darstellungsmangel
TFA02-006	indesign / illustrator / photoshop benutzen **distiller (aus pro dc)** für die Generierung PDFs für die Druckvorstufe (zB PDF/X-3) **inkscape** output prüfen (mit «inkscapeTest.svg/.pdf»). Resultat muss auf CLIMB Rechner in pro dc importiert/analysiert werden. Es ist nicht möglich, ein PDF mit den speziellen Randmarken und/oder Farbbändern für die Druckvorstufe zu produzieren.	Betriebsverhindernd
TFA02-007	indesign / illustrator / photoshop benutzen **distiller (aus pro dc)** für die Generierung PDFs für die Druckvorstufe (zB PDF/X-3) **gimp** output prüfen mit «GimpTest.pdf». Resultat muss auf CLIMB Rechner in pro dc importiert/analysiert werden. Es ist nicht möglich, ein PDF mit den speziellen Randmarken und/oder Farbbändern für die Druckvorstufe zu produzieren.	Betriebsverhindernd
TFA02-008	**pro dc unterstützt "plugins"**, bei Bern sind aktuell drei Plugins in Betrieb, je eines für Automatisierung, für Formulare und für "Tabellen". Auch «quite imposing plus» (siehe unten) ist ein Plugin. Es gibt keinen Support für Plugins unter Linux, Funktionalitäten müssten auf andere Weise bereitgestellt werden.	Betriebsverhindernd
TFA07-001	**reader dc: formulare ausfüllen** Mit Evince konnte das Testformular (PDFFormular.odt/.pdf) erfolgreich ausgefüllt werden.	Erfolgreich
TFA07-002	**reader dc: dokumente kommentieren** Auf dem jetzigen Linux-Client ist keine Software installiert, die sogenannte «Annotations» beherrscht. Es konnte nach dem Testen noch eine Open Source Software gefunden werden, die das kann: Icecream PDF Editor.	Betriebsverhindernd

TFB125	Testfall gehört eigentlich zu Pilot B: **quite imposing plus: (plugin zu pro dc):** "Ausschiessen", d.h. Seiten entfernen, umsortieren, neue Seitennummern, einzelne Bereiche "blanken", Druckbogen zusammenstellen Auf dem jetzigen Linux-Client ist keine Software installiert, die diese Anforderungen umsetzt Gemeinsam recherchiert und gewisse Tools gefunden: PDFsam, PDF-Shuffler, andere. Ein Feature konnte nach kurzer Durchsicht bei keinem der Tools gefunden werden: Neue Seitennummern) PDFsam ist bei der Stadt Bern bereits als Windows-Variante im Einsatz, kann aber zu wenig.	Betriebsverhindernd

4.3.2.2 TFA10 – Einschalttests von Crossover-Applikationen

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA10	**Banana Buchhaltung**	Erfolgreich

4.3.2.3 TFA11, 13, 14, 42 – Einschalttests von Citrix Applikationen

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA11	**Brother P-Touch Editor**	Erfolgreich
TFA13	**E3 (Zeitmanagement)** Problematisch war vor allem das Fensterverhalten	Betriebseinschränkend
TFA14	**Eiden Schichtenplaner**	Erfolgreich
TFA42	**SAP Logon PAD**	Darstellungsmangel

4.3.2.4 TFA12 Citrix Receiver

Für den Citrix Receiver wurde kein explizites Testszenario definiert. Implizit wurde dieser vor allem durch die zahlreichen Tests von Citrix-Applikationen im Pilot B getestet. Auch wurde ein grosser Teil der täglichen Arbeiten am Projekt auf Linux-Clients mit einem Citrix-Receiver durchgeführt.

Das grösste Manko ist aktuell die fehlende Unterstützung für SSO unter Linux. Ist man auf einem CLIMB-Client bereits eingeloggt, kann man ohne weiteres Passwort eine virtualisierte Applikation starten. Auf Linux braucht es immer zuerst einen Login mit dem Browser auf dem internen Citrix-Portal.

Das zweite Problem sind die zahlreichen «Darstellungsprobleme» (siehe 5.3.3.3.2 und 5.4.1). Aber auch diese können relativiert werden: Sie treten nur dann auf, wenn eine Applikation einzeln virtualisiert aufgerufen wird. Bei der Arbeit mit ganzen Desktop-Sessions treten diese nie auf. Letzteres wurde zwar nicht formal getestet, aber entspricht technisch der jetzigen Situation auf über der Hälfte der Arbeitsplätze (ThinClients mit Citrix-Viewer).

Die Funktion «Connection Center», in der die aktuell offenen Citrix-Applikationen und –Sessions angezeigt werden, steht in der Linux-Version nicht zur Verfügung. Diese ist für die Analyse von Problemen wichtig.

4.3.2.5 TFA18 / 24 / 25 / 41 Google Chrome/Microsoft Edge/Microsoft Internet Explorer/Oracle Java

Google Chrome ist auch für Linux verfügbar, ist dann aber nicht komplett OSS. Es wurde entschieden, lediglich Chromium (die OSS-Basis von Chrome) zu installieren und zu testen.

Ähnlich ist die Situation bei Java: Es gibt zwar das «Original»-Java von Oracle auch für Linux, aber diese ist nicht OSS. Auch hier wurde entschieden, mit OpenJDK ein reines OSS-Java zu installieren.

Microsoft-Browser gibt es nicht für Linux. Damit trotzdem ein zweiter Browser zur Verfügung steht, wurde Firefox auf dem Client zur Verfügung gestellt.

Für die Browser wurde kein explizites Testszenario definiert. Diese wurden jedoch implizit durch die Tests der zahlreichen Web-Applikationen getestet. Diese Tests von Pilot B (siehe 5.3.3.3.1) haben gezeigt, dass die OSS-Browser den Windows-Browsern ebenbürtig sind. Diese Aussage mag bei einer Erfolgsquote von nur 33% etwas gewagt wirken, aber die negativen Resultate dort betrafen nie die Browser selbst, sondern deren Umfeld (Webserver aus «normalem» Netz nicht erreichbar, Windows-Plugins, Office-Dokumente etc). Sofern man also von 100% «reinen» Web-Applikationen spricht, sind mit den OSS-Browsern keine bösen Überraschungen zu erwarten.

4.3.2.6 TFA27 – Microsoft Excel vs LibreOffice Calc

Die Tests von Excel waren weniger detailliert als die von Word (siehe nächstes Kapitel), aber das Fazit ist ähnlich: Sie haben kaum Unterschiede in der Funktionalität, sind aber untereinander "zu wenig kompatibel“, als dass man sie im täglichen Gebrauch jederzeit und mehrere Male hintereinander gegeneinander austauschen könnte.

Das bessere Resultat des Makro-Tests (TFA27-003 für Calc vs TFA34-005 für Writer) liegt eher an den unterschiedlichen Testfällen als an einer generell unterschiedlichen Unterstützung von Makros.

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA27-001	**Kompatibilität zu bestehenden Arbeitsmappen** "Buttons" haben unter LibreOffice nicht funktioniert (Migrationsproblem). Anbindung an Datenbank (direkt aus Excel) hat nicht funktioniert: Daten blieben zwar erhalten, wurden aber nicht mehr aktualisiert. "2018_Abfrage_GIS_DB.xlsm"	Betriebserschwerend
TFA27-002	**Pivottabellen** Erstellen von Pivottabellen problemlos. Bei Übernahme von Pivottabellen festgestellt: fehlendes Feature bei LibreOffice: MS Excel kann Pivot-Tabellen "zusammenfalten". Das hat in LibreOffice nach der Datenübernahme nicht mehr funktioniert. "2018_Abfrage_GIS_DB.xlsm"	Betriebserschwerend
TFA27-003	**Makro aufzeichnen / Makro programmieren / VBA** Basisfunktonalität, Übernahme von bestehenden Dokumente" Siehe auch verschiedene Anleitungen im Internet[5] [6]. Beispieldokument der Stadt Bern.	Erfolgreich
TFA27-004	**Funktionen für Formeln** Mit LibreOffice Extensions und Latex Elementen sehr umfangreich Beispieldokument der Stadt Bern	Erfolgreich
TFA27-005	**Schutz von Mappen, Blättern und Zellbreichen** Siehe auch im online[7].	Erfolgreich
TFA27-006	**PDF-Datei erstellen** Button	Erfolgreich
TFA27-007	**Rechtschreibung / Grammatik** Analog LibreOffice Writer	Erfolgreich

[5] https://help.libreoffice.org/Common/Recording_a_Macro/de

[6] https://wiki.documentfoundation.org/images/6/63/Makroprogrammierung_V41.pdf

[7] https://help.libreoffice.org/Common/Protecting_Content_in_LibreOffice

4.3.2.7 TFA34 – Microsoft Word vs LibreOffice Writer

Die ID der Stadt Bern bietet ihren Benutzenden einen umfassenden Basis Client mit dem auch Power User ihre Arbeit vollständig erledigen können. Mit einer OSS Lösung müssten die heute erfüllten Anforderungen weiter gewährleistet werden können.

Die Tests wurden von einer Mitarbeiterin der Stadt Bern definiert und dann gemeinsam mit Adfinis SyGroup AG durchgeführt. Die Bewertung wurde durch die Mitarbeiterin der Stadt Bern vorgenommen.

Zusammenfassend lässt sich sagen, dass der LibreOffice Writer über weite Strecken die Bedürfnisse einer Stadtverwaltung problemlos abdeckt: 13 erfolgreiche Tests und 5 mit "Darstellungsmangel“ stehen nur 4 "Betriebseinschränkend“ und 2 "Betriebsverhindernd“ gegenüber.

Die grosse Schwierigkeit einer Umstellung besteht nicht im Programm selbst, sondern am Austausch:

1. Arbeiten an einem gemeinsamen Dokument, abwechslungsweise mit Microsoft Word und LibreOffice, frustriert über kurz oder lang beide Seiten, weil immer wieder (eigentliche kleine) Dinge anders aussehen (z.B. Paginierung).
2. Es gibt viele Applikationen, die als Ausgabe- und Eingabeformat MS-Word-Dokumente erwarten. Im Inventar ist dies nicht erfasst, die Problematik wurde erst während des Testens ersichtlich.
3. Die Stadt Bern benutzt viele Vorlagen und Formulare auf Basis von MS-Word. Auch diese verhalten sich unter Umständen anders in LibreOffice und müssten zum grössten Teil angepasst oder sogar neu erstellt werden.

Beide Programme (MS Word und LibreOffice Writer) können jeweils das eigene und das "fremde“ Datenformat lesen und schreiben. Beide weisen praktisch dieselbe Funktionalität auf, normalerweise klappt auch die Übernahme von Dokumenten. Trotzdem sind sie untereinander "zu wenig kompatibel“, als dass man sie im täglichen Gebrauch jederzeit (und mehrere Male hintereinander) gegeneinander austauschen könnte.

Testfall Nr.	**Bezeichnung** Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	**Ergebnis / Bewertung**
TFA34-001	**Kompatibilität zu bestehenden Dokumenten** Komplexe, bestehende Dokumente testen Anwendungsbeispiel: Austausch mit externen Geschäftsstellen (mehrfach: .docx .odc) Test-Dokumente: "Outlook 2016 Einfuehrung.docx", "Word-Dokument mit allerlei Formatierungen-Bilder-Tabellen.docx"	Darstellungsmangel
TFA34-002	**Vorlagen-Handling (Vorlagen / meine Vorlagen)** Netzvorlagen, Eigene Vorlagen anhand mehrerer Beispiele testen Einige Formulare testen Test-Vorlagen: "Brief.dotm", "Kurzbrief.dotm" "Bericht A4 ID.dotx"	Darstellungsmangel

TFA34-003	**Vorlagen mit VBA** Mehrere Beispiele testen, Darstellung prüfen, Weiterverwendbarkeit prüfen Test-Vorlagen: "Brief.dotm", "Kurzbrief.dotm" "Bericht A4 ID.dotx"	Betriebsverhindernd
TFA34-004	**Formatvorlagen für Text oder Tabellen** Mehrere Beispiele testen Test-Vorlagen "Kurzbrief.dotm"	Darstellungsmangel
TFA34-005	**Makro aufzeichnen / Makro programmieren** Funktionalität vorhanden, Weiterverwendung bestehender Makros? Makros aus bestehenden Dokumenten funktionieren und werden bewahrt, sind aber nicht editierbar. LibreOffice - Tools - Options - Load/Save - VBA Properties. File muss wieder als MS-Office File gespeichert werden. Makros anpassen geht nur mit LibreOffice Basic Die Methoden und Objekte sind verschieden.	Betriebseinschränkend
TFA34-006	**Serienbrieffunktion** (Daten aus einer Address-Datei z.B. XLS / ACC / Word-Tabelle / OL-Kontakte usw.) Serienbriefe sind auch mit LibreOffice möglich, aber die Integration mit anderen Produkten ist anders gelöst. Konkret getestet mit Addresslisten aus .csv-Dateien. Testdokumente "Neues Dokument" ("Dokument") und alle Files im Verzeichnis "Serienbrief"	Betriebseinschränkend
TFA34-007	**Dokumente aus SAP** Steuerung aus SAP oder/und Fachapplikationen Erzeugte Dokumente aus SAP können problemlos in LibreOffice angezeigt werden, je nach Integration auf dem Desktop (Virtualisierung) öffnet sich aber automatisch das virtualisierte MS Word und nicht das lokal installierte LibreOffice	Betriebseinschränkend
TFA34-008	**Inhaltsverzeichnis / Index / Fussnoten / Quellenverzeichnis / Beschriftungen / Rechtsgrundlagenverzeichnis** Kompatibilität mit bestehenden Dokumenten Neues Dokument erstellen mit diesen Elementen	Erfolgreich
TFA34-009	**Überarbeitungsfunktionen / Änderungen nachverfolgen / Kommentare / Vergleichen / Bearbeitung einschränken** Kompatibilität mit bestehenden Dokumenten Austausch mit externen Geschäftsstellen Gegenseitig testen "Word-Dokument mit allerlei Formatierungen-Bilder-Tabellen.docx"	Erfolgreich

TFA34-010	**Verknüpfung zu anderen Programmen dynamisch** z.B. dynamischer Abgleich von .xlsx zu .pptx Erstelle spreadsheet und in Presenter: Insert - Object - OLE - from File… als Icon oder als Window auf der Seite Neues "Dokument1.docx"	Erfolgreich
TFA34-011	**Rechtschreibung / Grammatik / Thesaurus / Silbentrennung** Funktionalität vergleichbar mit Word? Alles moeglich, Tools - language, spelling, automatic spelling, thesaurus, etc DICs uebertragen & testen	Erfolgreich
TFA34-012	**Autokorrektur / Autoformat / Dokumentenprüfung / verschiedene Sprachen / Benutzer.dic** Funktionalität vergleichbar mit Word? Wiederverwendbarkeit von persönlichen Wörterbüchern (.dic) Alles moeglich, verwendet eigene Dics und persoenliche Dics moeglich. Kein Dokument (“Dokument1”)	Erfolgreich
TFA34-013	**Feldfunktionen / Textfelder** Vorgegebene Liste mit Word vergleichen Eigene Felder definieren Bestehende, eigene Felder weiterverwenden Felder (Fields) koennen direkt verglichen werden, Insert - Field - …More Fields… An bestehenden Files testen	Erfolgreich
TFA34-014	**Organigramme / SmartArts** Weiterverwendung bestehender Dokumente teilweise möglich, LibreOffice kennt zwar viele Symbols, Shapes, Charts etc. Es koennen auch LibreOffice Draw Objekte und alle Images verwendet werden. Bestehende Docs werden gut represäntiert.	Betriebsverhindernd
TFA34-015	**Suchen/Ersetzen/GeheZu von komplexen Formatierungen** LibreOffice: Edit - Find & Replace - Select "Format" or "Attributes" or "Paragraph Style" "Word-Dokument mit allerlei Formatierungen-Bilder-Tabellen.docx"	Betriebseinschränkend
TFA34-016	**Tabellen umwandeln / Text in Tabelle umwandeln** Format - Page - Header / Footer etc "Dokument1.docx"	Erfolgreich

TFA34-017	**Textmarken verwenden / Querverweise** - Auch Für VBA "Dokument1.docx"	Erfolgreich
TFA34-018	**Spezielle Kopf- und Fusszeilen (erste Seite anders / gerade/ungerade** Beispiel erstellen, bestehende Dokumente übernehmen Format - Page - Header / Footer etc "Outlook 2016 Einfuehrung.docx"	Erfolgreich
TFA34-019	**Grosse Dokument / Zentral- und Filialdokumente / Gliederung** LibreOffice: File - New - Master Document oder File - Open - choose existing File - Send - Create Master Document. Siehe auch online[8]. Verzeichnis “Zentraldokument”	Darstellungsmangel
TFA34-020	**Farbdesigns (CI / CD)** "Dokument1.docx"	Erfolgreich
TFA34-021	**Schnellbausteine / Textbausteine** Perfekt möglich. Suche in "Help" fuer "AutoText". Funktioniert. "Dokument1.docx"	Erfolgreich
TFA34-022	**Formeleditor** Im Formula Editor Formel eingeben. Wird sofort umgesetzt. "Dokument1.docx"	Erfolgreich
TFA34-023	**Dokumentenschutz (mittels Passwort wenn nötig)** Pro Dokument, einzelne Textfelder Siehe auch online[9]. (“Dokument1”) + “LO Passworttestx.docx/odt”	Erfolgreich
TFA34-024	**Entwicklertools für spezielle Formulare / Bearbeitung einschränken** (z.B. Radio button, Schaltflächen) Form Controls sind möglich: View - Toolbars - Form Controls "Dokument1.docx"	Darstellungsmangel

8 https://help.libreoffice.org/Writer/Working_with_Master_Documents_and_Subdocuments#Related_Topics

9 https://help.libreoffice.org/Common/Protecting_Content_in

4.3.2.8 TFA32 – Microsoft Powerpoint vs LibreOffice Impress

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA32-001	**Kompatibilität zu bestehenden Präsentationen** Getestet mit "ICT-Sicherheits-Schulung_NEU_16-9.pptx“	Erfolgreich
TFA32-002	**Datenimport OLE/DDE** "Präsentation1.pptx“	Betriebseinschränkend
TFA32-003	**Kiosk-Modus** Interaktive Präsentation "Präsentation1.pptx“	Erfolgreich
TFA32-004	Master / Farbschema "Präsentation1.pptx“	Erfolgreich
TFA32-005	**PDF-Datei erstellen** Button "Präsentation1.pptx“	Erfolgreich
TFA32-006	**Rechtschreibung / Grammatik** Analog LibreOffice Writer "Präsentation1.pptx“	Erfolgreich
TFA32-007	**Animationen** "Präsentation1.pptx“	Erfolgreich
TFA32-008	**Navigation mit Bluetooth Pointer** "Präsentation1.pptx“	Erfolgreich
TFA32-009	**Präsentation schützen** Umgesetzt gemäss online-Anleitung[10]. "Präsentation1.pptx“	Erfolgreich

4.3.2.9 TFA38 – Microsoft Visio vs LibreOffice Draw

Keine Tests definiert und durchgeführt.

[10] https://help.libreoffice.org/Common/Protecting_Content_in_LibreOffice

4.3.2.10 Native verfügbar

Nr	Testfall Titel Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	Bewertung
TFA04	Adobe Flash Player Ist neu auch im Browser (Chrome) integriert. Wird von Adobe gleichwertig für Windows/MacOS/Linux zum Download angeboten. End of life per 2020 angekündigt	Erfolgreich
TFA12	Citrix Receiver Gemäss Featurematrix[11] fehlen dem Citrix-Client für Linux einige Features, die bei Windows zur Verfügung stehen. Während der Tests wurden keine Defizite festgestellt ausser die SSO-Thematik und die Darstellungsprobleme. Siehe dazu auch 4.3.2.4.	Darstellungsmangel
TFA15	FileZilla (KAT2) Gemäss Webseite des Projekts gibt es keine Unterschiede zwischen der Windows- und der Linux-Version.	Erfolgreich
TFA16	Freemind Ist ein Java-Programm, die Windows- und Linuxversion unterscheiden sich deshalb nicht im Umfang.	Erfolgreich
TFA17	Gimp Gemäss Webseite des Projekts gibt es keine Unterschiede zwischen der Windows- und der Linux-Version.	Erfolgreich
TFA20	IDM UltraEdit (KAT2) Die Linux-Version hat nicht die selbe Versions-Nr wie die Windows-Version. Ob die fehlenden Features für die Stadt Bern relevant sind, ist mit Desk Research nicht zu klären. UltraEdit ist proprietäre Software.	Nicht durchgeführt
TFA21	Igor Pavlov 7-Zip 7-Zip ist open source software und umfasst für Windows und Linux dieselben Features.	Erfolgreich
TFA45	Trend Micro OfficeScan Agent XG Wird in dieser Form nicht benötigt.	Nicht durchgeführt

[11] https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-workspace-app-feature-matrix.pdf

TFA46	VLC Media Player VLC ist open source software und umfasst für Windows und Linux dieselben Features.	Erfolgreich
TFA47	Zope External Editor / OfficeConnector Das Produkt OfficeConnector wird nur für Windows und Mac angeboten. Es ist aber davon auszugehen, dass ein ähnlicher Komfort auch unter Linux zu erreichen ist. Ob eine entsprechende Lösung für die Stadt Bern brauchbar wäre, ist mit Desk Research nicht zu klären.	Nicht durchgeführt

4.4 Migrationszenario auf OSS

4.4.1 Erfüllung der Anforderungen

Beschränkt man die Betrachtung auf Software der Kategorie 1 und 2, dann können die meisten Benutzendenanforderungen mit einem Linux-Client und einer Mischung aus OSS- und kommerziellen Applikationen abgedeckt werden. Wie sich schon beim Installieren, aber spätestens bei den Benutzendentests herausgestellt hat, gibt es aber Defizite.

LibreOffice ist ein rundes, vollständiges Office-Paket. Trotzdem erfüllt es die Bedürfnisse der Stadt Bern nicht:

- Gemeinsames Entwickeln eines Dokuments ist in einem gemischten Team (Microsoft Office/Libre Office) kaum vernünftig möglich, viele kleine Fehler in der Formatierung beim Umwandeln summieren sich zu "zerrissenen“ Dokumenten.
- Es gibt einige (Web-) Applikationen, die direkt Microsoft-Office Dokumente konsumieren/produzieren. Diese müssten langfristig umgestellt werden auf LibreOffice – eine Arbeit für die wohl kaum ein Software-Hersteller ein Marktpotenzial sieht.

Applikationen wie E3 (Stundenerfassung) und SAP Logon PAD konnten nur virtualisiert zur Verfügung gestellt werden, eine lokale Installation mit Crossover war nicht möglich.

Aus den obgenannten Gründen wird die Benutzendenakzeptanz bei den meisten Anwendenden nicht gegeben sein.

4.4.2 Auswirkungen auf den IT Betrieb

Bei einer Umstellung auf einen Linux-Client zum jetzigen Zeitpunkt könnte auf virtualisierte Windows-Applikationen nicht verzichtet werden. Mindestens während einer Übergangszeit, potentiell auch "für immer", müsste die Stadt Bern das Windows Know-how und die Windows-Infrastruktur über weite Strecken beibehalten. Sie müsste also die Client-Plattform doppelt bereitstellen.

Die Gesamtkomplexität steigt durch diese doppelte Infrastruktur und damit tendenziell auch der Aufwand für Personal, Schulung und Sicherheit.

4.4.3 Vendor Lock In

Die Testresultate zeigen klar, dass ein Wechsel zu Linux auf dem Desktop zum jetzigen Zeitpunkt kaum möglich ist. Die Gründe

- Viele Applikationen sind **nur für Windows** verfügbar.
- Viele Dienstleistungen der Stadt Bern hängen von Office-Produkten ab –insbesondere von Microsoft Word. Es wurde über Jahre viel Aufwand in die Entwicklung von eigenen Templates und

Import-/Export-Schnittstellen zu anderen Applikationen investiert. Die **Datenformate** der Microsoft-Office-Palette sind theoretisch zwar offengelegt und könnten von Konkurrenzprodukten nachimplementiert werden. Praktisch gibt es aber nach wie vor so viele (kleine und grosse) Stolperfallen, dass die Zusammenarbeit an einem gemeinsamen Dokument abwechslungsweise mit Microsoft Word und LibreOffice Writer nicht zumutbar ist.

Der erste Punkt ist eine Frage des «Ökosystems» rund um eine Plattform. Da «alle» potentiellen Kunden bereits Windows als Ihr Desktop-Betriebssystem einsetzen, macht es für die Entwickler auch Sinn, nur für Windows zu entwickeln. Wie wichtig das Ökosystem rund um eine Plattform ist, sieht man daran, dass «Windows Mobile» (neben Android und IOS) praktisch bedeutungslos geworden ist: Weil es nur sehr wenige Apps für Windows Mobile gibt, will auch niemand so ein Mobiltelefon kaufen.

Je grösser ein «Ökosystem» rund um eine Plattform ist, desto mehr Vertrauen geniesst die Plattform und sie kann noch einfacher noch grösser werden. Die Stadt Bern kann das Ökosystem rund um Linux (als Desktop-Betriebssystem) nicht merklich beeinflussen. Aber sie könnte die Abhängigkeit von Windows Schritt für Schritt lösen, indem sie bei Neu-Anschaffungen konsequent nur noch Web-Applikationen akzeptieren würde. Diese könnten dann auf einem beliebigen Gerät mit Web-Browser bedient werden, egal ob das ein Windows-Rechner, ein Apple-iPad oder ein Android-Handy ist.

Der zweite Punkt ist eine Frage der Datenformate, die verwendet werden. Bei der Diskussion um Open Source Software werden oft nur die Programme betrachtet. Mindestens so wichtig ist aber das Format der Daten. Offene Datenformate brauchen mindestens eine offengelegte Spezifikation (bei .docx der Fall) und eine definierte Hoheit über das Format – es muss sich weiterentwickeln können. Liegt diese Hoheit bei einer einzelnen Firma, dann besteht immer das Risiko, dass diese das Format in eine unerwünschte Richtung lenkt. Dies ist zum Beispiel bei PDF (Adobe) und DOCX (Microsoft) der Fall. Diese Konstellation ist gerade für Konkurrenten ziemlich unattraktiv, da sie zwangsläufig immer «hinterherhinken». Solche Formate sind der Form nach «open», aber das wichtigste Versprechen von OSS halten sie nicht ein: Wenn man sich substantiell beteiligt, kann man auch etwas beeinflussen. Wirklich offen sind nur Formate, welche einen gemeinschaftlichen Ansatz zur Steuerung verfolgen, wie zum Beispiel ODT (OASIS).

Der Vendor Lock-In besteht aus dem einmaligen Migrations-Aufwand von bestehenden (und weiter benutzten) Ergebnissen (wie Dokumentvorlagen) und dem wiederkehrenden Aufwand beim Austausch mit anderen Stellen.

Ein schrittweiser Wechsel des Dokumentenformats in einer Organisation ist nicht attraktiv, da man so dauernd mit kleineren und grösseren Baustellen innerhalb der Organisation rechnen müsste. Bei einer Umstellung auf einen Schlag hat man anfänglich einen sehr grossen Aufwand (und das beträchtliche Risiko, dass nicht alle Applikationen umgestellt werden können) und dafür intern keine Probleme mehr – aber die Probleme im Austausch mit anderen Stellen bleiben.

4.5 Kostenvergleich

4.5.1 Szenario

OSS Basis Client und 40 wichtigste Applikationen (Kat. 1+2)

- **Annahme**: 20% der 2500 User würden den Linux Client und LibreOffice nutzen, also 500 Clients
  - Kat.1
    - Applikationen nativ (keine Kosten)
    - 12 Applikationen alternativ (v.a. LibreOffice)
  - Kat. 2
    - 4 Applikationen alternativ
    - Restliche Applikationen wie Kat. 3 über XenDesktop eingespielt

4.5.2 Investitionen

- **Engineering/Systemaufbau**: Konzeption, Automatisierung, Integration

    - **Annahme**: Interne Aufwände bewegen sich in derselben Grössenordnung wie die externen Aufwände
    - Das Ausrollen von 500 Clients wurde nicht berechnet, da dieses bei der nächsten Migration auch bei Windows anfallen würde
    - Citrix-Receiver, Integration in den Linux Desktop wurde einberechnet (auch für Pilot B relevant)
- **Einmallizenzen**: Nicht relevant
- **Migration**: Migration von Vorlagen berechnet mit folgenden Annahmen
    - **Annahme**: 100 Vorlagen
    - Aufwand pro Vorlage ca. 3-4 Stunden
- **Betreiberschulung**: Es wurden folgende **Annahmen** getroffen
    - Office Support: 6 Personen der Stadt, 3 Tage Schulung
    - Client OS Support: 6 Personen der Stadt, 3 Tage Schulung
    - Deployment / Backendserver Support: 4 Personen der Stadt, 2 Tage Schulung
- **Benutzendenschulung**: Insbesondere im Bereich Office erheblich. Aber auch beim Linux Desktop.
    - 1 Tage Desktop und wichtigste Applikationen
        - 500 User
    - 1 Tag Office, das wären 4-6 Stunden mehr, als ein Refresh, der auch mit MS Office geplant wäre
        - 500 User, je einen halben Tag
        - durchgeführt durch die Stadt selber in Klassen zu 10 Personen
    - Grafikprogramme (Kat 2)
        - 100 – 300 User von Adobe Grafikprogramme
            - Annahme: 20% wechseln auf den Linux Desktop und Alternative Software wie Scribus oder Inkscape/Blender
        - Schulungsaufwand pro Applikation 2 Tage

Pilot A: Investitionen

		Zusätzliche Investitionen Aufbau OSS Plattform												
		Administratoren / Support Schulung			Engineering / Systemaufbau			Migration (Daten / Schnittstellen)			Benutzer-schulung			Total
Bereich		int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT 4)			0			0			0			0	0
	Basisapplikationen (KAT 1 und KAT 2)			0	80	200	51'600	400	200	98'000	1'280	240	233'600	383'200
	Office Suite (KAT 1)	144	72	35'280	200	200	69'000	300	50	53'500	2'440	32	299'200	456'980
	Betriebssystem	144	72	35'280	700	700	241'500	0	0	0	4'440	40	540'800	817'580
	Hardware			0			0			0			0	0
Netzwerk	WAN			0			0			0			0	0
	LAN			0			0			0			0	0
Data Center	WEB Applikationen			0			0			0			0	0
	Virtualisierungs-plattform			0			0			0			0	0
	SW Deployment	64	48	18'880	500	500	172'500			0			0	191'380
	Zentrale Applikationen			0			0			0			0	0
	Datenbank			0			0			0			0	0
	HW / Server / OS			0			0			0			0	0
	RZ Raum/Strom/Klima			0			0			0			0	0
Total				89'440			534'600			151'500			1'073'600	1'849'140

4.5.3 Betriebskosten

- **Subscriptions**: Der Desktop kann prinzipiell ohne Subscriptions betrieben werden. Es gibt allerdings Angebote, die auch den Desktop abdecken würden. In jedem Fall empfiehlt sich sowieso eine Form von externer Unterstützung durch einen Spezialisten

- Linux (z.B. Ubuntu): 500 Desktops x 150 CHF / Jahr = ca. 75'000 CHF
- Für LibreOffice empfiehlt sich ein Support-Packet und SLA. In dieser Grössenordnung ca. 45'000 CHF / Jahr
- Alle weiteren Applikationen würden wir nicht mit Subscriptions abdecken
- Die Backend-Infrastruktur wurde mit vier RHEL-Servern gerechnet

- **Admin/Support-Aufwand**
  - Interne Betriebsaufwände sind für uns kaum abzuschätzen. Hier wären Vergleichszahlen der Stadt notwendig.
  - Sollte nach einer Einführungsphase in etwa gleich hoch sein, wie für eine CSS Plattform
  - Im Szenario mit dem Betrieb von zwei Plattformen gleichzeitig, reduziert sich allerdings der Aufwand auf der einen Seite nicht so stark, wie er auf der anderen Seite ansteigt. Deshalb das Delta, das sich weniger aus dem Support, sondern aus der Pflege des zusätzlichen Software Stacks erklärt.

Pilot A: Betriebskosten

		Reduktion bisheriger Betriebsaufwand / Jahr						Zusätzlicher Betriebsaufwand OSS / Jahr				Vergleich
		Lizenzen		Admin / Support			Total	Subscriptions	Admin / Support		Total	
Bereich		Anzahl	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]	ext. [CHF]	int. [h]	[CHF]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT 4)					0	0			0	0	0
	Basisapplikationen (KAT 1 und KAT 2)					0	0			0	0	0
	Office Suite (KAT 1)	-500	-42'720	0		0	-42'720	45'000	500	72'500	117'500	74'780
	Betriebssystem	-500	-26'645	0		0	-26'645	75'000	1200	174'000	249'000	222'355
	Hardware					0	0			0	0	0
Netzwerk	WAN					0	0			0	0	0
	LAN					0	0			0	0	0
Data Center	WEB Applikationen					0	0			0	0	0
	Virtualisierungs-plattform					0	0			0	0	0
	SW Deployment					0	0	3'040	300	43'500	46'540	46'540
	Zentrale Applikationen					0	0			0	0	0
	Datenbank					0	0			0	0	0
	HW / Server / OS					0	0			0	0	0
	RZ Raum/Strom/Klima					0	0			0	0	0
Total			-69'365			0	-69'365	123'040		290'000	413'040	343'675

4.6 Zusammenfassung

4.6.1 Ergebnisse

Im Rahmen des Projekts CLIMB, der Erneuerung der Client Plattform der Stadt Bern wurden ca. 2/3 der festen Arbeitsplätze auf Thin Clients umgestellt. Dies sind LINUX - basierte Geräte und sie verfügen somit bereits heute über ein OSS Betriebssystem. Aus verschiedenen Gründen (Mobilität, Leistung, spezielle Hardware) sind nach wie vor ca. 800 FAT Clients im Einsatz (Desktops oder Notebooks).

Im Pilotprojekt A konnte ein OSS Client mit den wichtigsten Eigenschaften eines professionellen Arbeitsplatzes weitgehend automatisiert von der "leeren" Hardware aufgebaut werden. Er verfügt über die notwendigen Funktionalitäten wie Globale Einstellungen, Single Sign on Internet Browser und Citrix Receiver.

Mit einem externen Security Audit wurde festgestellt, dass nicht alle notwendigen Härtungsmassnahmen umgesetzt waren. Gleichzeitig wurde festgehalten, dass der OSS Client so aufgesetzt werden kann, dass er den Sicherheitsvorgaben der Stadt Bern entspricht. Security Features umfassen unter anderem

Screenlock, Disk Encryption, Firewall, Antivirus Software und die Möglichkeit, regelmässig Security Patches und Updates einzuspielen.

Libreoffice als OSS Alternative zu Microsoft Office genügt weitgehend den Bedürfnissen der Anwendenden. Ist ein Datenaustausch mit anderen Stellen erforderlich oder müssen Daten von Fachapplikationen exportiert oder importiert werden, ist dies nur sehr erschwert möglich. Dies stellt das grösste Hindernis für den Einsatz von Libreoffice dar.

Der Basis Client bietet 30 Applikationen (KAT 1) als Grundausstattung. Es handelt sich dabei um verbreitete Funktionalitäten, weshalb 20 OSS Alternativen gefunden werden konnten. Gründliche Tests zeigten jedoch auf, dass viele dieser OSS Alternativen Einschränkungen aufwiesen, so dass sie für den professionellen Einsatz nicht genügten ("betriebsverhindernd"). 8 OSS Alternativen können mit Einschränkungen für den Betrieb eingesetzt werden.

Die 17 Applikationen der KAT2 bieten Grundfunktionalitäten an wie z.B. Visio oder MS Project. Hier wurden 3 Native und 7 OSS Alternativen getestet. Von letzteren hat sich lediglich eine Applikation als geeignet erwiesen.

4.6.2 Chancen

Der Einsatz von OSS anstelle von proprietärer Software bietet im Pilotprojekt A folgende Chancen:

- Teilweises Lösen der Abhängigkeit von marktdominanten Herstellern (Microsoft)
- Erster Schritt in eine Langzeitstrategie der Lösung von dominanten Herstellern
- Intuitivere Benutzendenoberfläche (z.B. Libreoffice vs. MS Office)
- Bei einem kleineren OSS Support Anbieter wahrscheinlich stärkerer Kundenfokus spürbar
- Keine Formatumwandlung bei der Langzeitarchivierung

4.6.3 Risiken

Der Einsatz von OSS anstelle von proprietärer Software birgt im Pilotprojekt A folgende Risiken:

- Dokumentenaustausch mit anderen Abteilungen oder externen Stellen ist aufgrund des nicht identischen Datenformats nicht durchgängig
- Dies erzeugt Mehraufwand, Produktivitätsverlust und Unzufriedenheit bei den Benutzenden
- Schnittstellen zu Fachapplikationen müssen mit entsprechendem Aufwand angepasst werden. Dies wird voraussichtlich nicht für jede Fachapplikation möglich sein
- Neue Abhängigkeit von kleineren, auf OSS Produkte spezialisierten Unternehmen
- Parallelbetrieb von zwei Client-Plattformen ist technisch komplexer und damit fehleranfälliger

4.6.4 Finanzen

- Einsparung von Microsoft Windows Lizenzen: ca. 27 KCHF / Jahr
- Einsparung von Microsoft Office Lizenzen: ca. 43 KCHF / Jahr
- Investitionen für den Plattform Aufbau: 535 KCHF
- Investitionen für den Know-how Aufbau (inkl. Interne Kosten): 1'073 KCHF

4.6.5 Empfehlung

- Kein Wechsel auf den OSS Basis Client, da er als primärer bzw. einziger Arbeitsplatz nur für wenige Mitarbeitende brauchbar ist
- Die steigenden Kosten lassen sich nicht mit entsprechendem Mehrwert rechtfertigen
- Libreoffice als Alternative unter Windows anbieten

4.6.6 Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Der Dokumentenaustausch mit internen und externen Stellen ist nicht durchgängig.
Sicherstellen des stabilen Informatikbetriebs	Die Stabilität kann mit dem Aufbau von Know how sichergestellt werden. Die Komplexität des Betriebs nimmt zu.
Wirtschaftlichkeit	Die Investitionen in den Plattformaufbau führen zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden. Ein erster Schritt wäre möglich. Gleichzeitig können neue Abhängigkeiten zu kleineren, auf OSS Produkte spezialisierten Firmen entstehen.

5 Pilotprojekt B: Fachapplikationen

5.1 Anforderungsdefinition

Die Stadtverwaltung Bern umfasst eine Vielzahl von Funktionen, welche von den einzelnen Abteilungen wahrgenommen werden. Deren Mitarbeitende sind auf Fachapplikationen angewiesen, mit welchen sie ihre täglichen, spezialisierten Aufgaben abwickeln.

Die Fachapplikationen werden von den Abteilungen für ihre speziellen Bedürfnisse ausgewählt und beschafft. Die ID der Stadt Bern stellt die Applikationen auf den Clients der Mitarbeitenden zur Verfügung. Dies umfasst eine Liste von ca. 180 Applikationen.

Diese Applikationen werden nicht von einem breiten Publikum verwendet. Aus diesem Grund finden sich für Fachapplikationen in der Regel weder direkt vom Hersteller dieselbe Applikation für Linux («OSS Native») oder eine Alternative. Aber es gibt schon eine KAT3-Web-Applikation, welche die Stadt Bern als OSS entwickeln liess (zum Beispiel TFB045).

Für jede Fachapplikation ist ein Applikationsverantwortlicher zuständig. Der Applikationsverantwortliche definierte die notwendigen Tests und führte diese mit Unterstützung eines Spezialisten von Adfinis SyGroup durch.

5.2 Umsetzung

5.2.1 Lösungsansatz

Wo es beim Pilot A um die mehr oder weniger flächendeckend eingesetzte Client-Software geht, sind bei Pilot B die sogenannten Fachapplikationen das Thema. Für Fachapplikationen gibt es (auch ausserhalb der Stadt Bern) eine deutlich geringere Nachfrage.

Bei reinen **Software**-Lösungen, wo theoretisch Open Source Produkte relativ einfach möglich wären, gibt es schon alleine wegen der geringen Verbreitung nur wenige potentielle unabhängige Entwickler. Andere Fachapplikationen sind "nur" Hilfsprogramme zum Betrieb spezialisierter **Hardware**. So gibt es unter anderem eine Applikation zur Programmierung von autarken Modulen für die Gebäudeautomatisierung, ein Zutrittskontroll-System mit Bild- und Tonübertragung sowie Türöffnern, oder eine Überwachungs/Steuerungs-Software von Kassenautomaten bei Parkhäusern. Hier ist es praktisch unmöglich, dass es unabhängige Entwickler gibt - macht doch die Software nur Sinn im Zusammenspiel mit hochspezialisierter, teurer Hardware und muss erst noch bei jedem Hardware-Release angepasst werden. Auch ist die Kernkompetenz von Herstellern solcher Lösungen oft die Hardware und nicht die Desktop-Software.

Es ist also bei Fachapplikationen nicht davon auszugehen, dass es eine Open-Source Variante gibt. Auch ist es für die Hersteller kaum lukrativ, selber eine (auch closed source) Linux-Version bereitzustellen.

Trotzdem wurde für die meisten Applikationen beim Hersteller recherchiert, ob er die Software auch für andere Plattformen bereitstellt. Das Ergebnis war mehr oder weniger wie erwartet: Über die Hälfte der Hersteller schreibt auf der Webseite nicht einmal, dass nur Windows unterstützt wird – so selbstverständlich ist das. Bei anderen findet man immerhin eine Liste der unterstützten Windows-Versionen.

Aus diesen Gründen wurde beschlossen, die Priorisierung der möglichen Implementationen im Vergleich zu Pilot A zu verändern: Die Applikationen, die jetzt schon nur (Citrix-) virtualisiert zur Verfügung stehen, werden ausschliesslich als Citrix-Applikation getestet.

5.2.2 Aufbau der Infrastruktur

Für Pilot B wurde die Infrastruktur weiterbenutzt, die für Pilot A aufgebaut wurde. Es wurden lediglich zusätzliche Applikationen auf dem Client berücksichtigt.

5.2.3 Installation Basis-Client

Der Client von Pilot A konnte unverändert übernommen werden, es mussten lediglich zusätzliche Software-Pakete bereitgestellt und die Konfiguration für die zu installierenden Pakete angepasst werden.

5.2.4 Installation der Applikationen

Um herauszufinden, wie eine Applikation auf einem Open Source Client installiert werden soll, war das Vorgehen bei Kat1/2 Applikationen im Pilot A wie folgt: Zuerst Native, dann Alternative suchen. Dann mit Crossover versuchen und schliesslich der Fallback auf Citrix.

Nach den Erfahrungen im Pilot A haben wir für Pilot B den Ablauf angepasst. Es war schon bei den Kat1/2-Applikationen klar, dass es für einige wenige Applikationen keinen Weg gab, diese direkt auf Linux zum Laufen zu bringen. Bei Fachapplikationen war diese Problematik bei einem deutlich grösseren Anteil der Applikationen zu erwarten. Sollte also die Stadt Bern komplett auf einen Linux-Client umstellen, müsste sie trotzdem eine Windows-Infrastruktur für die Ausführung der "Problem-Applikationen" bereithalten.

Aus diesem Grund war die Reihenfolge bei Kat3 Applikationen wie folgt:

Ist die Applikation jetzt lokal installiert?

- Falls ja, gleiches Vorgehen wie bei Kat1/2 (Also Native/Alternative/Crossover/Citrix-Applikation).
- Falls nein (d.h. sie wird jetzt schon ausschliesslich als Citrix-App bereitgestellt), dann bleiben wir bei Citrix-Applikation (keine weiteren Analyse).

Wir haben für alle (über 60) lokal installierten Applikationen recherchiert, ob es dieselbe ("nativ") oder eine ähnliche ("alternativ") Software gibt. Dabei gab es mehrere Hindernisse:

- In wenigen Fällen konnte allein aus dem Namen der Software keine Herstellerpräsenz im Internet ausgemacht werden.
- Bei den restlichen hat nur etwa die Hälfte der Seiten explizit die unterstützten Plattformen aufgelistet. Ohne explizite Angaben sind wir davon ausgegangen, dass lediglich Windows unterstützt wird.

Schliesslich haben wir bei diesen Applikationen nur drei gefunden, die sich als "native" oder als "Alternative" umsetzen liessen:

Atos CardOS gibt es gemäss Hersteller nativ für Linux. Dies ist keine eigentliche Applikation, sondern ein Treiber/Hilfsprogramm zur Ansteuerung einer Smartcard. Dies wird benutzt, um Dokumente zu signieren und/oder verschlüsseln. Dies war leider im Inventar der Applikationen so nicht ersichtlich, sondern wurde erst während der Tests ersichtlich.

Notepad++ (vielseitiger Texteditor): Es gibt dutzende Texteditoren nativ für Linux. Da das Testszenario zum Zeitpunkt der Paketierung nicht zur Verfügung stand, haben wir eine Umsetzung mit Crossover gemacht. Aus Sicht Betriebssystem ist ein Texteditor auch eine "einfache" Applikation, d.h. die Chancen für eine erfolgreiche Crossover-Umsetzung stehen sehr gut.

Quite Imposing (Tool, welches auf Basis von "Acrobat pro DC" PDFs manipuliert): Es gibt viele Tools unter Linux um PDFs zu manipulieren. Auch hier gab es zum Zeitpunkt der Paketierung kein Testszenario, welches eine Evaluation von Alternativen erlaubt hätte.

Bei der Installation mit Crossover haben wir uns (Aufwand/Ertrag) entschieden, "nur" die etwa 35 Applikationen zu implementieren und testen zu lassen, die 5 und mehr berechtigte User haben. Die restlichen gut 25 Applikationen werden das Bild nicht mehr wesentlich verändern (siehe dazu auch 5.3.3 und insbesondere 5.3.3.1.2).

5.2.5 Bereitstellen der Daten

Die Applikationsverantwortlichen haben selbst die benötigten Daten definiert und bei den Tests benutzt.

5.2.6 Konfiguration Infrastruktur

Es wird dieselbe Infrastruktur wie bei Pilot A verwendet.

5.2.7 Funktionstest

Wie im Pilot A bereits beschrieben, gab es bei den Applikationen, die mit Crossover bereitgestellt wurden, schon im Rahmen der Paketierung einen kurzen Test: Startet die Applikation oder nicht?

Die Applikationen, die via Citrix-Portal getestet wurden, konnten wegen der Berechtigungen im Voraus nicht getestet werden (sonst hätten einzelne Projektmitarbeitende die Berechtigung zur Ausführung sämtlicher Kat3-Applikationen benötigt).

5.3 Testdurchführung

5.3.1 Grundsätzliche Lösungsansätze

5.3.2 Native, Alternative, Crossover, Citrix-Applikation

Kat-3 Applikationen sind hoch spezialisierte Anwendungen, welche von den einzelnen Direktionen der Stadt Bern selber verantwortet werden. Es liegt in der Natur der Sache, dass nur für wenige dieser Applikationen native Versionen oder alternative Software vorliegen. Wie in Pilot A ist die Fallback-Variante die Citrix-Applikation. Einige Kat-3 Applikationen liegen aber bei der Stadt Bern (noch) nicht als Citrix-Applikation vor, diese müssen dann in der Regel als "Crossover“-Applikation implementiert werden.

5.3.3 Testfälle pro Applikation

Das Inventar der Stadt Bern, das für diese Analyse zur Verfügung stand, umfasst total 184 KAT3 Applikationen. Ein (kleiner) Teil davon muss nach wie vor «von Hand» auf den Clients installiert werden (früher «KAT4»).

Wegen der Menge der Applikationen und dem vorhandenden Budget war von vornherein klar, dass nicht alle Applikationen analysiert werden konnten und deshalb eine Auswahl nötig sein wird. Bei den ausgewählten Applikationen wurde maximal ein Testdurchlauf mit den Applikationsverantwortlichen durchgeführt, es gab keine Nachbesserung nach den Tests. Die Applikationen wurden also zuerst triagiert und dann die entsprechenden Tests mit den Applikationsverantwortlichen organisiert.

Ohne Test mit AV (72)

- 24 Applikationen: Zu wenige User (hat nur «**lokale**» Applikationen betroffen). Keine Wertung.
- 25 Applikationen: **Lokale** Applikationen, bei denen ein Crossover-Packaging erfolglos versucht wurde. Da für diese keine Citrix-Variante zur Verfügung steht, kann mit den AVs nicht getestet werden. Muss als Fehlschlag gewertet werden.
- 23 Applikationen: **Citrix**-Applikationen, für die zwar ein Test geplant war, der aber nicht durchgeführt werden konnten. Gründe dafür waren Abwesenheiten der AVs, Applikation funktioniert bekanntermassen auch schon mit Windows/Citrix nicht genügend gut, Inventarfehler, etc.

Termin mit AV durchgeführt (112):

- 14 Applikationen: **Lokale** Applikationen, bei den das Crossover-Packaging technisch funktioniert hat. Alle Applikationen ausser notepad++ haben unter Crossover versagt. Die anderen sind aus diversen Gründen gescheitert (Abhängigkeiten zu Spezialhardware oder anderer Software,

Firewalleinstellungen, Inventarfehler, …). Es ist davon auszugehen, dass diese Quote deutlich gesteigert werden kann, aber nur mit einem Aufwand von mehreren Tagen pro Applikation.

- 33 Applikationen: Web-Applikationen, von denen 11 erfolgreich getestet wurden. Die anderen zwei Drittel sind gescheitert. Gründe dafür waren unter anderem Firewall-Sperren (Applikation ist nur aus spezifischen Netzwerken erreichbar, nicht aus dem Testnetz) oder Abhängigkeiten zu Microsoft Office-Produkten oder Browser-Plugins, die nur für Windows verfügbar sind.
- 65 Citrix Applikationen, davon
  - 32 erfolgreich
  - 19 (9 «Darstellungsmängel», 10 «Betriebseinschränkend») hatten mit mehr oder weniger grossen Darstellungsproblemen (oder fehlenden gemeinsamen Shares) zu kämpfen, welche aber mit mehr Aufwand als behebbar eingeschätzt werden.
  - 14 wurden als «betriebsverhindernd» gewertet, Ursache waren massive Darstellungsprobleme und Abhängigkeiten zu Spezialhardware.

5.3.3.1 Kein Test durchgeführt (72)

5.3.3.1.1 Nicht getestet weil zu wenige User (24)

Die meisten Applikationen mit (gemäss Inventar) höchstens 3 Usern sind zur Zeit rein lokale Installationen (d.h. nicht über Citrix verfügbar), einige können auch nur zusammen mit Spezialhardware vor Ort sinnvoll eingesetzt werden.

Testfall-Nr.	Bezeichnung Weitere Bemerkungen	Anzahl User
TFB004	**Anapol ChipDrive 4.0.6**	3
TFB013	**AutoDesk AutoCAD**	1
TFB019	**Bausys Bausoftware Hydraulik 4.1**	3
TFB029	**Canon Capture Perfect** INC60805, läuft nur auf CLiPx und nicht CLIMB.	0
TFB030	**Canon image FORMULA DR-G1130**	3
TFB032	**Cinema 4D**	
TFB035	**CLX.ClubMaker**	
TFB042	**DHI MikeUrban 2014**	3
TFB044	**Dürr Scanner (DBSWIN)**	
TFB046	**Dynasphere HSR Managing Tool 1.0**	1
TFB049	**EJPD eBiometrie-RichClient 37264** Braucht Spezialhardware vor Ort, kann nicht getestet werden	1
TFB051	**EJPD Interpol I-24/7** Fehler im Inventar?	
TFB064	**Epson VISA Printer**	2

	Braucht Spezialhardware vor Ort, kann nicht getestet werden. Wird benutzt zusammen mit eBiometrie RichClient	
TFB068	**Flexysign**	3
TFB075	**Hager EG003 2.0.1**	
TFB078	**HP DeskJet**	
TFB083	**InfoRapid Suchen und Ersetzen 3.1**	0
TFB086	**Kaiser DataSwiss Vote**	3
TFB093	**Kofax**	1
TFB099	**Luxor Display Q**	2
TFB110	**Nuance Dragon NaturallySpeaking**	2
TFB167	**Tools4Ever UMRA Console 10.4**	2
TFB177	**x64 Image Driver**	
TFB182	**Zwahlen Zeiterfassung 2.63**	1

5.3.3.1.2 Nicht getestet (keine Citrix-Version und Crossover Install erfolglos) (25)

Wie bei den meisten KAT3-Applikationen, wurden auch für diese Applikationen keine mit Linux kompatiblen Versionen oder Alternativen gefunden.

Testfall-Nr.	Bezeichnung	Anzahl User
TFB017	Avedris New Paka	8
TFB031	Centro Digital Smart Client 17.1.0.0	5
TFB040	C-Trace c-ware Map Europa City 2013	14
TFB065	ErgoDent Firma CCS (Nachfolge Dent-II)	69
TFB072	GISBern GIS-Suite V 5.0	88
TFB089	KaPo MACS-B 3.9.25	107
TFB105	Microsoft SQL Server Managementstudio 2012	9
TFB108	Nemetschek Vectorworks 2017	40
TFB114	Onyx RIP Thrive 211	3
TFB115	OnyxCeph	33
TFB120	PTV VisionVissim 5.4	9
TFB121	PTV VisionVissim 8	
TFB129	Romexis (Kaladent)	34
TFB134	SAP Analysis	24
TFB140	SEA easy access	6

TFB141	SEA easy access 1.1.55.10638	6
TFB149	Stadtverwaltung Bern Adrus1.3.54	28
TFB151	Stadtverwaltung Bern GemDat 5.375.37	108
TFB152	Stadtverwaltung Bern GemDat 5.435.43	115
TFB163	Stadtverwaltung Bern Submiss 1.5.0.1	57
TFB169	Uptime ArtsClient 3.3.14.2	69
TFB171	Verkehrs-Systeme AGVS-WorkSuite 3.0.9	9
TFB173	WebDev Swiss Pension 6	15
TFB178	Xplain eneXs	7
TFB179	Xplain Gerätesoftware-Regula 7024.M110	7

5.3.3.1.3 Citrix: Nicht durchgeführte (kein Resultat) und nicht durchführbare (23)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	**Ergebnis / Bewertung**
TFB003	**Aidex KeyOrganizer 6.11** (7) Gemäss AV sind es mittlerweile noch zwei Berechtigte User (aber er gehört nicht dazu).	Nicht durchführbar
TFB009	**Atos CardOS 5.3** (104) Siehe dazu auch TFB058	Nicht durchgeführt
TFB014	**Avam Appgate 10.2.2.0** (4) AV war nicht verfügbar	Nicht durchgeführt
TFB022	**Bentley MicroStation 10** (34) Fehler im Inventar, Applikation unter Citrix nicht verfügbar	Nicht durchführbar
TFB023	**Bentley MicroStation 8.11.7** (11) Fehler im Inventar, Applikation unter Citrix nicht verfügbar	Nicht durchführbar
TFB025	**Biella Schweiz Dominal Print 2** (2) Applikation ist ein Starter für eine Microsoft Access Datei (O:\...\xxx.mdb). Das kann so nicht funktionieren.	Nicht durchführbar
TFB061	**Entsorgung und Recycling ERB Follow Me Editor** (4) AV war nicht verfügbar	Nicht durchgeführt
TFB062	**Epsilon Avedris** (22) AV war nicht verfügbar	Nicht durchgeführt

TFB063	**Epson Scan** (14) AV war nicht verfügbar Epson bietet in der Regel auch Linux-Treiber für Ihre Scanner an, Support abhängig von den konkret verwendeten Modellen.	Nicht durchgeführt
TFB091	**Kieback & Peter LOYTEC** (1) AV war nicht verfügbar	Nicht durchgeführt
TFB096	**LOBOS 3.x** (85) AV war nicht verfügbar	Nicht durchgeführt
TFB101	**Maxon Cinema 4D11.5** (1) Keine Binaries geliefert, kein Test möglich	Nicht durchführbar
TFB104	**Microsoft SCOM Console** (7) Fehler im Inventar, wird auf Clients nicht mehr angeboten	Nicht durchführbar
TFB106	**Mobatime TachoPlus 1.2** (2) AV war nicht verfügbar	Nicht durchgeführt
TFB113	**OM ComputerOM Mannschaft 04.04.150828** (11) Fehler im Inventar, wird nicht mehr verwendet	Nicht durchführbar
TFB126	**Real VNC VNC5.0.3** (2) AV war nicht verfügbar	Nicht durchgeführt
TFB130	**RR-Projekt 2.14.2 R-Project 2.14.2** Ist gemäss AV auch mit Citrix unter Windows deutlich zu wenig performant, Test mit Citrix unter Linux ist deshalb nicht sinnvoll.	Nicht durchführbar
TFB131	**Safenet Sentinel HASP5.95** Gemäss AV eine Dongle-Lizenzsoftware. AV war nicht verfügbar	Nicht durchgeführt
TFB137	**SAS 9.4** Ist gemäss AV auch mit Citrix unter Windows deutlich zu wenig performant, Test mit Citrix unter Linux ist deshalb nicht sinnvoll.	Nicht durchführbar
TFB138	**SBU DATAVER Abwasser 3** (45) Gemäss AV noch nicht unter Citrix verfügbar	Nicht durchführbar
TFB144	**Siedle ASHT 3.2.12.0** (28) Kann gemäss AV nur vor Ort getestet werden, muss direkt mit Telefonanlage verbunden sein.	Nicht durchführbar
TFB164	**Suva Gefahren Portfolio 1.3.0.0** (3) AV war nicht verfügbar	Nicht durchgeführt

TFB166	**Swissmentor MD8.0.1** (2) AV war nicht verfügbar	Nicht durchgeführt

5.3.3.2 Zu Tests eingeladene Lokale Applikationen (Crossover) (14)

Alle fehlgeschlagen oder kein Resultat, ausser Notepad++

TFB002	**ABB Obelisk 3.6.1** (2) bringt USB-Gerät mit Nur Windows, USB Gerät wurde nicht erkannt. Sehr wahrscheinlich bräuchte dies einen spezifischen Linux-Treiber (es reicht nicht wenn der Treiber in Crossover installiert wird)	Betriebsverhindernd
TFB005	**AnkerPC Cashcontrol 1.0.1** (19) Test wegen fest installierter Hardware (Kassensystem, serielle Schnittstelle) nicht möglich	Nicht durchführbar
TFB008	**Atos CardOS 5.3** (106) Ist Voraussetzung für die SSO-Lösung vom EJPD. Konnte mangels Kartenlesegerät und Berechtigung vor dem AV-Termin nicht getestet werden. Müsste wahrscheinlich nativ unter Linux installiert werden. Kein Testresultat, wird zusammen mit TFB011 «gezählt»	Betriebsverhindernd
TFB011	**Atos CardOS API 5.3** (106) Siehe oben TFB008	Betriebsverhindernd
TFB016	**AVAYA Contact Center Manager CCM 7** (11) Ist eigentlich eine Web-Applikation. Wurde aber hier getestet, weil der heikle Punkt die Abhängigkeit vom Silverlight-Plugin ist.	Betriebsverhindernd
TFB021	**Bentley InRoads 39394** (7) Ist abhängig von TFB022. TFB022 sei gemäss Inventar virtualisiert, dies stimmt aber gemäss AV nicht.	Nicht durchführbar
TFB054	**EJPD ISR** (101) Abhängig von TFB008.	Betriebsverhindernd
TFB058	**EJPD SSO Portal 3.0.2** (106) Abhängig von TFB008. Die Installation mit Crossover ist erfolgreich durchgelaufen und kann gestartet werden, aber die Web Site, die geöffnet werden soll, öffnet sich nicht (Firewall?). Gemäss Polizeiinspektorat ist das Portal via Citrix zwar verfügbar, funktioniert aber (auch dort) nicht richtig	Betriebsverhindernd
TFB059	**EJPD Vostra** (101)	Nicht durchführbar

	Abhängig von TFB008. Kann nicht getestet werden, da Testperson vereidigt sein muss.	
TFB095	**Land Software Entwicklung Lidos** (15) wurde abgelöst, nicht mehr in Betrieb.	Nicht durchführbar
TFB109	**Notepad++** (25) Funktioniert sowohl unter Crossover als auch unter Citrix.	Erfolgreich
TFB124	**Q-SysRAI Soft 40028** (41) Wurde nicht paketiert, da keine Binaries zur Verfügung gestellt werden konnten.	Nicht durchführbar
TFB125	**Quite Imposing Plus2.1** (6) Mit Crossover konnte kein installierbares Paket erzeugt werden. Test unter Citrix nicht möglich, weil AV lediglich lokale Variante benutzt und keine Berechtigung für Citrix-Version hat (siehe auch Pilot A, Kapitel 4.3.2.1)	Nicht durchführbar
TFB176	**Woodwing SmartStyles** (5) Fehler im Inventar (Keine Lizenz mehr)	Nicht durchführbar

5.3.3.3 Test mit AV durchgeführt (98)

5.3.3.3.1 Web-Applikationen (33)

Zusammengefasst gab es für die 33 Web-Applikationen, die getestet werden sollten, folgende Resultate

- 11 Erfolgreich
- 1 Betriebseinschränkend (Gemäss AV funktioniert Sharepoint zwar über weite Strecken auch in einem OSS Browser, aber es gibt immer noch einzelne Punkte, die «mühsamer» sind).
- 17 Betriebsverhindernd (Windows-Plugins, Interaktionen mit Office-Produkten, Firewall und SSO Probleme, …)
- 2 nicht durchführbar (Inventarfehler, Firewall)
- 2 ohne Resultat (Einladung AV kam nicht zustande)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	**Ergebnis / Bewertung**
TFB006	**ApA**	Erfolgreich
TFB015	**AVAYA Agent Desktop** (14) Plugin kann nicht installiert werden (verlangt explizit IE 10 or higher)	Betriebsverhindernd
TFB018	**Basler & Hofmann AG Stratus 5** (?) Applikation hat an sich funktioniert, aber der Arbeitsschritt "Export zu Excel, Bearbeiten in Excel, Import aus Excel" hat mit LibreOffice Calc nicht funktioniert, da LibreOffice beim fixed	Betriebsverhindernd

	space export anscheinend die falsche Spaltenbreite setzt (und die Extension immer .csv und nicht .txt ist).	
TFB024	**BFS Eidg.Gebäude und Wohnungsregister** (?)	Erfolgreich
TFB027	**Bund UPI Viewer** (?)	Erfolgreich
TFB028	**Bundesamt für Sozialversicherungen BSV Telezas 3** (?)	Erfolgreich
TFB034	**Citrix GoToAssyst** (24)	Betriebsverhindernd
TFB048	**EJPD Arkila** (?)	Betriebsverhindernd
TFB050	**EJPD iFado Produktion** (?)	Betriebsverhindernd
TFB052	**EJPD Intranet Schengen / SIRENE** (?)	Betriebsverhindernd
TFB053	**EJPD Intranet SEM** (?)	Betriebsverhindernd
TFB055	**EJPD JMessageHandler** (?) Kein Zugriff	Betriebsverhindernd
TFB056	**EJPD Nevis IDM** (?)	Betriebsverhindernd
TFB057	**EJPD Ordipro Web** (?) Ordipro Web ist eine Applikation vom EDA und ist nicht im EJPD-Portal enthalten.	Betriebsverhindernd
TFB060	**EJPD ZEMIS** (?)	Betriebsverhindernd
TFB080	**IGK Industrie- und Gewerbekataster Bern und Basel** (?)	
TFB084	**iWeb RBS** (?)	Erfolgreich
TFB085	**Jean-Baptiste Simmen CSE IT Solutions SA CSE KIBE** (?) Der Browserteil hat Problemlos funktioniert. Die Applikation produziert aber komplexe Excel Files mit Makros (kleine Applikationen mit Login zu DB). Diese DB-Files funktionieren in LibreOffice Calc nicht.	Betriebsverhindernd
TFB087	**Kanton Bern GRUDA AV** (?)	Erfolgreich
TFB088	**Kanton Geres** (?) Konnte nicht getestet werden (Firewall Issue)	Nicht durchführbar
TFB094	**KöR** (?) Funktioniert nur mit Firefox (braucht Java)	Erfolgreich
TFB097	**LOGO** (?) Ist keine Web-Applikation, sondern wird als EXE von einem Share gestartet (!)	Betriebsverhindernd
TFB098	**Löwenstein & Partner NIL** (?)	Erfolgreich
TFB117	**PM Plus+** (?)	Erfolgreich
TFB123	**QMPilot** (?)	Erfolgreich
TFB127	**redM Software VSS-Reader** (1)	Nicht durchführbar

	Kann nicht getestet werden, es gibt nur 1 User (aber das ist nicht die applikationsverantwortliche Person)	
TFB132	**SAMA** (?) Ist keine Web-Applikation, sondern wird als EXE von Share gestartet.	Betriebsverhindernd
TFB135	**SAP CRA** (?)	Betriebsverhindernd
TFB142	**SharePoint** (?) Funktioniert im Wesentlichen, aber die volle Funktionalität (zB in Browser "Word") nur mit MS Browser.	Betriebseinschränkend
TFB146	**Staatssekretariat für Wirtschaft SECO Lamda** (?) Applikation des Bundes	Nicht durchgeführt
TFB147	**Stadtplan** (?)	Erfolgreich
TFB172b	**wmware Webclient (6.5)** (15) Einige wichtige Funktionalitäten gibt es nur als Flash-Plugin, z.B. das Netapp Plugin (notwendig für das Management von Snapshots, Restores, …)	Betriebsverhindernd
TFB174	**Web-GIS** (?)	Betriebsverhindernd

5.3.3.3.2 Citrix (65)

Da die Bereitstellung der virtualisierten Citrix-Applikationen im Rahmen des Piloten B keinen Engineering-Aufwand nach sich zieht und lediglich einen lokalen Citrix-Client und einen Benutzenden mit entsprechender Berechtigung voraussetzen, wurde bei den Citrix-Applikationen auch dann ein Test geplant, wenn die Anzahl Benutzenden unbekannt oder weniger als 5 waren.

5.3.3.3.2.1 Getestet «Erfolgreich» (32)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	**Ergebnis / Bewertung**
TFB001	**AAC Infotray Limsophy 9.2** (20)	Erfolgreich
TFB026	**Bixi Atlaxy 1.6.70.20** (13)	Erfolgreich
TFB033	**Cisco Security Manager Client 4.6.0 SP1** (4) nicht mehr Lokal (nur auf Citrix) Beim Starten der Applikation gab es eine Fehlermeldung vom X. Jedoch wurde die Applikation trotzdem gestartet	Erfolgreich
TFB036	**CMI AXIOMA Alle 4.26.2474** (350)	Erfolgreich
TFB043	**Docuteam Packer** (5)	Erfolgreich
TFB045	**DV Bern E-BEGU** Braucht einen USB-Barcode/QR-Scanner	Erfolgreich

	Ist unter dem Namen Ki-Tax auf dem GitHub-Account der Stadt Bern zu finden[12].	
TFB047	**Educate IT Raptor Client 3.6.7** (190)	Erfolgreich
TFB066	**Erne Polipoint PEP 37166** (61)	Erfolgreich
TFB074	**Grupet UNTIS Stundenplan 2012** (5)	Erfolgreich
TFB076	**Hess Management Console ERB Fellerstrasse** (8)	Erfolgreich
TFB077	**Hess Management Console ERB Schermenweg** (7)	Erfolgreich
TFB081	**Infogate eCase Schuldensanierung 10.0.1.9** (5)	Erfolgreich
TFB090	**Keepass KeePass2.23** (245)	Erfolgreich
TFB100	**M&S antecura 1029.001** (12)	Erfolgreich
TFB111	**Objectif LunePrintShop Mail7.2.7 Multilanguage** (11)	Erfolgreich
TFB112	**OM ComputerOM Bauten-Zupla 04.08.160713** (7)	Erfolgreich
TFB119	**Predata WinMedio** (5)	Erfolgreich
TFB122	**Putty Putty 0.62** (48)	Erfolgreich
TFB139	**Schneider Winbau 16.9** (29)	Erfolgreich
TFB143	**SIA Reader 2.4.5.2** (34)	Erfolgreich
TFB148	**Stadtverwaltung Bern Adrus1.3.54** (45)	Erfolgreich
TFB150	**Stadtverwaltung Bern Damispez 1.1.3**	Erfolgreich
TFB156	**Stadtverwaltung Bern KliBur-NG 1.2.15.0** (9)	Erfolgreich
TFB157	**Stadtverwaltung Bern NSB-Nameneditierung 1** (7)	Erfolgreich
TFB158	**Stadtverwaltung Bern NSB-Reports 1** (71)	Erfolgreich
TFB159	**Stadtverwaltung Bern Pegasus 1.4.3.1**	Erfolgreich
TFB160	**Stadtverwaltung Bern Progress 1.2.6** (13)	Erfolgreich
TFB162	**Stadtverwaltung Bern Submiss 1.5.0.1** (117)	Erfolgreich
TFB175	**WinFEE FEE 4.0**	Erfolgreich
TFB180	**Zebra GC420t 2.2.3** (32)	Erfolgreich
TFB181	**Zebra TLP2844 1.1.9.1048**	Erfolgreich
TFB184	**Ian Opac**	Erfolgreich

[12] https://github.com/StadtBern

5.3.3.3.2.2 Getestet «Darstellungsmangel» (9)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	Ergebnis / Bewertung
TFB038	**Commend ComWin 3.1.5200.14** (26)	Darstellungsmangel
TFB041	**Devolution RemoteDesktopManager RDPM 11.1.0** (20) Es gibt native Linux-Alternativen (rdesktop, ssh, vncviewer, …) Implementation wäre stark von den tatsächlich benötigten Protokollen abhängig.	Darstellungsmangel
TFB079	**IBO QSR8.5.4** (8)	Darstellungsmangel
TFB133	**SAP Analysis** (56)	Darstellungsmangel
TFB136	**SAP Design Studio**	Darstellungsmangel
TFB153	**Stadtverwaltung Bern Gewepo 4.9.0** (67)	Darstellungsmangel
TFB155	**Stadtverwaltung Bern In4mer Admin 1.0** (8)	Darstellungsmangel
TFB172a	**vmwarevSphere Client 5.1.0** (15) Die Citrix-Variante ist technisch ein Chrome Browser mit Flash auf Citrix	Darstellungsmangel
TFB183	**Filezilla** Wurde hier als Citrix-Applikation getestet, kommt auch native in Pilot A vor (siehe 4.3.2.10)	Darstellungsmangel

5.3.3.3.2.3 Getestet «Betriebseinschränkend» (10)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	Ergebnis / Bewertung
TFB037	**CMI CMIStar** (18) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend
TFB069	**Formica Baumschulsoftware** (2) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend
TFB071	**Geocom HO33-201733-2017** (7) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend
TFB102	**Microsoft (Navision) Betreuungsgutscheine** (17) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend
TFB107	**MPS FIM Friedhofsmanagement** (31) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend

TFB116	**Philipp Kirsch Datanet 4.5** (11) Datenimport ab USB-Stick funktioniert nur via Workaround (Testclient stellt noch nicht alle gemeinsamen Laufwerke zur Verfügung)	Betriebseinschränkend
TFB128	**Robin Stuart ZINT 2.4.3.0** (12) Ein Netzlaufwerk hat gefehlt (Testclient stellt noch nicht alle gemeinsamen Laufwerke zur Verfügung Erzeugen QR-Code funktioniert nur, wenn explizit ZINT aufgerufen wird, nicht auf Doppelclick im Explorer.	Betriebseinschränkend
TFB145	**Sierzega grs 5.2** (3) Ein Netzlaufwerk hat gefehlt (Testclient stellt noch nicht alle gemeinsamen Laufwerke zur Verfügung	Betriebseinschränkend
TFB168	**Tools4Ever UMRA Form 10.4** (23) Gemäss Testprotokoll grössere Darstellungsprobleme	Betriebseinschränkend
TFB185	**Sierzega SR4** Ein Netzlaufwerk hat gefehlt (Testclient stellt noch nicht alle gemeinsamen Laufwerke zur Verfügung Konnte nicht getestet werden, geht wegen speziellen Lizenzen nur auf lokalen PCs.	Betriebseinschränkend

5.3.3.3.2.4 Getestet «Betriebsverhindernd» (14)

Testfall Nr.	**Bezeichnung** (Anzahl User wenn bekannt) Weitere Hinweis zu Testdurchführung	**Ergebnis / Bewertung**
TFB012	**Atos CardOS API 5.3** (104) SSO-Portal kann ohne TFB009 (Atos Card OS API 5.3) nicht geöffnet werden;	Betriebsverhindernd
TFB020	**BBT Software AGSunet Plus 5.2016.03.2049** (31) Gemäss Testprotokoll massive Darstellungsprobleme.	Betriebsverhindernd
TFB039	**Conject Conject FM 8.2.0.7** (22) Gemäss Testprotokoll massive Darstellungsprobleme (z.B. «Mauszeiger ca. 2cm zu hoch», erst nach mehrmaligem Herumklicken und Wechseln zwischen den Tabs stimmt der Mauszeiger). Ungeplant wurde die Applikation auch noch als Web-Applikation getestet (Ergebnis: kleinere Darstellungsprobleme)	Betriebsverhindernd
TFB067	**Filemaker FileMaker 13 Pro** (14)	Betriebsverhindernd

	Gemäss Testprotokoll massive Darstellungsprobleme (z.B. startet sehr langsam oder erst nach dem zweiten, dritten Versuch)	
TFB070	**Frox Atiras Client 7.0.4** (10) Zunächst Darstellungsprobleme (weil Applikation noch in zweiter Citrix- Session am Arbeitsplatz offen war). Danach soweit ok, bis «einfrieren» nach Abruf der Verkehrsdaten.	Betriebsverhindernd
TFB073	**Google SketchUp Pro8** (8) Gemäss AV zu alte Version in Citrix. Import-/Zugriff auf Modelle funktioniert nicht (evtl «Ein Netzlaufwerk hat gefehlt»?)	Betriebsverhindernd
TFB082	**Infogate eCase Schulsozialarbeit 9.0.14.15** (17) Ein Netzlaufwerk hat gefehlt (Testclient stellt noch nicht alle gemeinsamen Laufwerke zur Verfügung	Betriebsverhindernd
TFB092	**KiSS Integration 4.5** (497) Gemäss Testprotokoll sehr oft falsche Fehlermeldungen (obwohl kein Problem besteht) und Probleme im Full-Screen Betrieb. Applikation öffnet externe Word- und Excel-Dateien.	Betriebsverhindernd
TFB103	**Microsoft Dynamics NAV Classic 2009R2 6.0.32012.0** (160) Gemäss Testprotokoll massive Darstellungsprobleme («Beim Erstellen eines Berichtes (Vorschau) verschiebt sich das Hauptfenster auf den zweiten Bildschirm und friert ein. Die Applikation muss danach geschlossen und wieder geöffnet werden»)	Betriebsverhindernd
TFB118	**PMI Scolaris 4.50.2** (144) Applikation beruht auf Microsoft Access Applikation friert reproduzierbar ein, sobald der Bildschirm gewechselt wird.	Betriebsverhindernd
TFB154	**Stadtverwaltung Bern Gewepo Reports 1.0.21** (15) Applikation beruht auf Microsoft Access Teil "Märkte und Stände" hat problemlos funktioniert. Teil "Taxi" hatte bei den "Firmenkarten" nur das Template gezeigt, aber nicht die Daten aus der DB.	Betriebsverhindernd
TFB161	**Stadtverwaltung Bern Spicon 2.0.0** (173) Gemäss Testprotokoll massive Darstellungsprobleme	Betriebsverhindernd
TFB165	**Swiss SignSuisse ID 3.7** (59) Karte wurde nicht gefunden, weder mit Word noch mit SuisseID localsigner	Betriebsverhindernd

TFB170	**Verkehrs-Systeme AGVS-WorkSuite 3.0.9** (50) Gemäss AV funktioniert unter Windows/Citrix die Applikation zwar, ist aber letztlich zu langsam für den täglichen Gebrauch. Läuft nur wenn Dongle (Schlüssel) gefunden werden kann (via USB, läuft dann auf Server)	Betriebsverhindernd

5.4 Migrationszenario auf OSS

5.4.1 Erfüllung der Anforderungen

Was die Resultate der KAT1/KAT2 Applikationen im Pilotprojekt A vorgezeichnet haben, hat sich bei der Software KAT3 mehr als bestätigt:

Bei **Crossover** funktioniert zu oft schon die Installation nicht. Es ist zwar davon auszugehen, dass mit mehr Zeitaufwand mehr Applikationen auch unter Crossover zum Laufen gebracht werden könnten, aber auch, dass es bei einigen gar nie funktionieren wird. Zudem leisten die Hersteller von Windows-Software nur dann Support, wenn sie wie spezifiziert unter Windows läuft. Die Stadt Bern hat in den letzten Jahren intensiv daran gearbeitet, möglichst alle Applikationen virtualisiert zur Verfügung stehen. Diest ist ein weitere Erklärung für das sehr schlechte Resultat von Crossover: Es mussten vor allem übrig gebliebene, also «schwierig zu integrierenden Applikationen» mit Crossover zum Laufen gebracht werden.

Virtualisierte Applikationen («**Citrix-Applikationen**») laufen im Citrix-Receiver unter Linux recht gut. Trotz kleineren und grösseren Problemen gab es nie Datenverlust. Zum Beispiel wurden Fenster unerwartet minimiert, das heisst sie verschwanden vom Bildschirm, aber waren noch in der Task-Leiste. Oder es konnte eine vertikale Differenz von einigen cm zwischen der angezeigten und der tatsächlichen Position des Mauszeigers beobachtet werden. Einige dieser Probleme verschwanden, nachdem die Testperson die Instanz der Applikation, die noch auf Ihrem CLIMB-Client lief, geschlossen hatte. Andere traten nur dann auf, wenn die Applikation im Vollbildschirm angezeigt wurde. Die Testpersonen haben diese Probleme unterschiedlich beurteilt, von «Darstellungsmangel» bis zu «Betriebsverhindernd». Weiter könnte bereits der Aufruf über das Web-Portal anstelle eines transparenten Starts über die Task-Leiste als «Darstellungsmangel» oder noch schlechter bewertet werden.

Die meisten Web-Applikationen haben gut funktioniert, leider gibt es auch hier noch einige Beispiele, welche wegen ihrer (veralteten) Architektur nur in Browsern auf Windows lauffähig sind (z.B. mit einem Silverlight Plugin).

5.4.2 Auswirkungen auf den IT Betrieb (gleich wie Pilot A)

Bei einer Umstellung auf einen Linux-Client zum jetzigen Zeitpunkt könnte also auf virtualisierte Windows-Applikationen nicht verzichtet werden. Mindestens während einer Übergangszeit, potentiell auch "für immer", müsste die Stadt Bern das Windows Know-how und die Windows-Infrastruktur über weite Strecken beibehalten. Sie müsste also die Client-Plattform doppelt bereitstellen.

Die Gesamtkomplexität steigt durch diese doppelte Infrastruktur und damit tendenziell auch der Aufwand für Personal, Schulungen und Sicherheit.

5.4.3 Vendor Lock In

Bei KAT3-Applikationen besteht der Vendor-Lock-In im Wesentlichen aus denselben zwei Komponenten wie bei KAT1/2:

- **Ökosystem**: Gerade Anbieter von Software, die deutlich weniger verbreitet ist (zum Beispiel Steuerung von Kassenautomaten in Parkhäusern im Vergleich zu Microsoft Word), sehen kaum

eine Möglichkeit, die zusätzlichen Aufwände für eine weitere Client-Plattform zu refinanzieren und bieten deshalb keine Linux-Variante an.

- **Datenformate**: Die Problematik der proprietären Formate ist bei KAT3-Software geringer als bei KAT1/KAT2, da es deutlich weniger Altdaten gibt. Trotzdem ist der Austausch mit externen Stellen auch hier wichtig (zum Beispiel Druckvorstufe).

5.5 Kostenvergleich

5.5.1 Szenario

Der Pilot B deckt Fachapplikationen ab, die sich in den allermeisten Fällen nur auf Windows betreiben bzw. benutzen lassen. Der Versuch der Cross-Kompilierung ist gescheitert. Auf einem Linux-Client liessen sich diese Applikationen nur "einbinden", indem ein Windows Desktop über Citrix XenDesktop eingebunden wird.

5.5.2 Investitionen

- **Engineering/Setup:**
  - Client: Einbindung SmartCard-Lösungen (diverse)
  - Web-Applikationen: Kaum Aufwand. Wenig für Testing, allenfalls für Drucker, VPN-Zugänge etc.
  - XenDesktop: Single-Sign-On, Darstellungsprobleme (siehe Pilot A), Drucken
  - Keine Aufwände beim Software Deployment

Pilot B: Investitionen

		Zusätzliche Investitionen Aufbau OSS Plattform												
		Administratoren / Support Schulung			Engineering / Systemaufbau			Migration (Daten / Schnittstellen)			Benutzer-schulung			Total
Bereich		int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT 4)			0			0	400	200	98'000			0	98'000
	Basisapplikationen (KAT 1 und KAT 2)			0			0			0			0	0
	Office Suite (KAT 1)			0			0			0			0	0
	Betriebssystem			0	40	120	29'800	100		14'500			0	44'300
	Hardware			0			0			0			0	0
Netzwerk	WAN			0			0			0			0	0
	LAN			0			0			0			0	0
Data Center	WEB Applikationen			0	160	40	31'200			0			0	31'200
	Virtualisierungs-plattform			0	60	200	48'700			0			0	48'700
	SW Deployment			0			0			0			0	0
	Zentrale Applikationen			0			0			0			0	0
	Datenbank			0			0			0			0	0
	HW / Server / OS			0			0			0			0	0
	RZ Raum/Strom/Klima			0			0			0			0	0
Total				0			109'700			112'500			0	222'200

5.5.3 Betriebskosten

- Keine zusätzlichen Betriebskosten für Fachapplikationen der Kategorie 3 und 4 auf dem Linux Client

5.6 Zusammenfassung

5.6.1 Ergebnisse

Für die proprietären Fachapplikationen der Stadt Bern gibt es heute keine "Native" OSS Lösung. OSS-Lösungen gibt es vereinzelt und nur bei Web-Applikationen (z.B. Ki-Tax, TFB045). Auf einem OSS Client können die virtualisierten Applikationen (Citrix) und die WEB Applikationen grösstenteils betrieben werden. Es gibt jedoch auch hier einen Teil Fachapplikationen, die auf einem OSS Client nicht funktionieren.

5.6.2 Chancen

Die Tatsache, dass viele Fachapplikationen im Rahmen des Projekts CLIMB virtualisiert wurden, führt dazu, dass diese gemäss unseren Tests auch auf einem OSS Basis Client benutzt werden können. Sie stellen somit kein Hindernis für die Einführung eines OSS Basis Client (Pilot A) dar.

Bei den Fachapplikationen besteht die Hauptchance darin, bei neu zu beschaffende Fachapplikationen die Kompatibilität zum OSS Client zu fordern.

Im Fall einer Neuentwicklung als OSS Applikation könnte sie zusammen mit den Fachdiensten anderer öffentlicher Verwaltungen entwickelt werden.

5.6.3 Risiken

Die Nutzung von Fachapplikationen auf einem OSS Client birgt folgende Risiken:

- Web-Applikationen, die nur für einen bestimmten Browser unter Windows entwickelt wurden, werden nicht korrekt dargestellt oder funktionieren nicht.
- Gewisse CITRIX Fachapplikationen funktionieren nicht oder nicht einwandfrei
- Für Fachapplikationen, welche lokal unter Windows installiert werden müssen, gibt es kaum eine Lösung mit Crossover. Sie können nicht mit einem OSS Client genutzt werden.
- Crossover wird von den Applikationsherstellern nicht unterstützt und verunmöglicht damit einen professionellen Einsatz

5.6.4 Finanzen

- Keine Einsparmöglichkeiten
- Kleine Investitionen für die Anpassung der Plattformen (Citrix, WEB) verbessern die Nutzbarkeit der virtualisierten Fachapplikationen.

5.6.5 Empfehlung

- OSS Clients könnten ausschliesslich für diejenigen Mitarbeitenden eingesetzt werden, deren Fachapplikationen auf einem Browser oder unter Citrix einwandfrei funktionieren (keine betriebseinschränkenden Mängel und keine Darstellungsmängel). Dies bleibt aber wegen der Empfehlung von Pilot A ein theoretisches Gedankenspiel.
- Die OSS-Browser sollten daher bereits bei den Beschaffungen Beachtung finden. Der Support von Web-Applikationen durch den Hersteller ist sicherzustellen.

5.6.6 Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Die Fachapplikationen können teilweise auf einem OSS-Client benutzt werden. Heute gibt es kaum OSS-Alternativen.

Sicherstellen des stabilen Informatikbetriebs	Die Stabilität des IT Betriebs wird nicht verändert.
Wirtschaftlichkeit	Es sind Investitionen erforderlich. Sie führen jedoch zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden.

6 Pilotprojekt C: Groupware

6.1 Anforderungsdefinition

Funktionale Anforderungen

Die Kern-Funktionen einer Groupware sind E-Mail (mit Adressbüchern[13]) und Kalender. Weitere Funktionen sind Tasks und Notizen, deren Benutzung ist aber je nach Person sehr unterschiedlich.

Betriebliche Anforderungen

Die ID der Stadt Bern betreibt aktuell eine Exchange-Infrastruktur im eigenen RZ ("on premise") mit Outlook als Client-Software. Die wichtigste Anforderung aus Betreibersicht ist die Verfügbarkeit: der Betrieb "steht still" ohne Groupware.

6.2 Umsetzung

6.2.1 Lösungsansatz

Wie eingangs erwähnt, hat die Stadt Bern beschlossen, die Lösungen in der eigenen Infrastruktur aufzubauen. Beim Mail-System kam dazu, dass die Verfügbarkeit des Groupware-Systems hoch sein muss. Als Projektänderung wurde beschlossen, einen redundanten Aufbau zu demonstrieren.

Es gibt aktuell mehrere OpenSource Produkte, welche als Ersatz für Microsoft Exchange in Frage kommen. Da es zu Beginn keinen detaillierten Anforderungskatalog gab, hat Adfinis SyGroup aufgrund der eigenen Erfahrungen das Produkt "Open Xchange“ für die Demo-Installation bei der Stadt Bern ausgewählt. Einerseits ist dieses Produkt bei Internet-Providern im grossen Stil im Einsatz (das heisst es gibt eine grosse Basis an bestehenden Installationen), andererseits hat eine vergleichende Requirements Analyse Ende 2016 bei einem Kunden mit ca 30‘000 Postfächern Open Xchange als "bestes“ OSS-Produkt ergeben. Obwohl die Anforderungen dieses Kunden mit der Stadt Bern nicht deckungsgleich sind, war das doch einer der Gründe für die Wahl von Open Xchange, Dort ist dieses System jetzt über ein Jahr erfolgreich im Einsatz.

6.2.2 Aufbau der Infrastruktur

Im Gegensatz zum Pilot A/B, wo die Test-Clients im produktiven Netz installiert wurden, wurde für den Groupware-Test entschieden, ein abgetrenntes Netz zu verwenden. Der Hauptgrund dafür war, dass nicht auszuschliessen war, dass OX allenfalls Schema-Änderungen am verwendeten Active Directory (AD) brauchen würde. Eine Schema-Änderung (mit zusätzlichen Attributen) ist zwar einfach und risikoarm durchzuführen, aber eine solche zurückzunehmen (also die zusätzlichen Attribute wieder zu entfernen) ist ziemlich heikel. Es war schnell klar, dass die Stadt Bern ein separates Test-AD aufbauen muss.

6.2.2.1 Serverübersicht

Die Kernkomponente von OX ist der "OX-Server". Dieser stellt die gesamten Groupware-Funktionalitäten (Kalender, Adressbücher, ...) zur Verfügung. Folgende Komponenten sind ebenfalls wichtig für die Implementation bei der Stadt Bern:

Web-Frontend (entspricht OWA)

Mailstore: Die Basis-Mail-Funktionalität (ohne Groupware-Spezifika) wird vom OX Server über IMAP/LMTP bezogen. Als Serverkomponente kommt "Dovecot" zum Einsatz. Hier werden neben den

[13] Damit sind sowohl zentrale Addressbücher, die aus dem zentralen Verzeichnis zur Verfügung gestellt werden als auch die von den Anwendenden selbst gepflegten Kontakte gemeint.

eigentlichen Mails auch einige mailbezogene Benutzendeneinstellungen wie zum Beispiel Abwesenheitsmeldungen, Weiterleitungen, etc gespeichert (SIEVE).

AD (LDAP): Hier sind Benutzende und das globale Adressbuch zu finden. Read only für OX.

mySQL Datenbank: Hier werden die Kalendereinträge, die persönlichen Adressbücher der Benutzenden etc gespeichert.

File Store: Einige wenige persönlichen Benutzendendateien werden direkt als Dateien abgelegt.

Die Komponenten werden jeweils einzeln hochverfügbar gemacht.

Weitere Hinweise zur Architektur von OX-Systemen sind online[14] zu finden.

6.2.3 Installation der "Applikationen"

Im Rahmen der Tests wurde der Web-Client von OX genauer untersucht. Deshalb braucht es lediglich einen Browser auf dem Client.

6.2.4 Bereitstellen der Test-Daten

Für diesen Piloten braucht es keine speziellen Test-Daten, diese werden bei den Testläufen erzeugt.

6.2.5 Anbindung der Schnittstellen

Von aussen ansprechbar sind ausschliesslich die Frontend-Server über https.

OX-HTTPS (Web-Frontend): Wie diese gegen aussen HA verfügbar gemacht werden, war nicht mehr Teil der Pilot-Installation, hier kommt jeder gängige https Load-Balancer in Frage, in einer einfachen Implementation kann das auch einfach DNS-Round-Robin sein.

OX-EAS (Zugriff mit "Exchange Active Sync"): HA analog OX-HTTPS.

SMTP (Anlieferung neue Mails): Ebenfalls auf den Frontend-Servern, d.h. auch hier wird HA analog OX-HTTPS gelöst.

6.2.5.1 Mailversand

SMTP (Versand neue Mails): Je nach konkretem Anwendungsfall werden Mails sowohl von den OX Frontend-Servern als auch von den Dovecot-Backend-Servern versendet.

Authentisierung: Benutzende werden beim Login gegen einen der beiden AD-Server geprüft.

6.2.5.2 Provisioning

OX benutzt interne User Accounts, es reicht nicht wenn die Accounts im AD vorhanden sind. Den Prozess, Mutationen an Usern ("Joiner/Leaver/Mover") im AD automatisch entsprechend im OX-System zu aktualisieren, nennen wir in diesem Zusammenhang Provisioning. Im Rahmen des Piloten wurde das Provisioning manuell gelöst, d.h. Test User wurden manuell sowohl im AD als auch in OX angelegt.

In einer produktiven Implementation müssen die Benutzenden automatisch angelegt (umbenannt, gelöscht) werden können. Eine Automatisierung sollte sich möglichst schlank in die bestehenden Prozesse einfügen, OX bietet zum Beispiel ein SOAP-API an, über welches Benutzende verwaltet werden können.

[14] http://oxpedia.org/wiki/index.php?title=AppSuite:Architecture_Overview

6.2.5.3 Integration MDM

Im Rahmen des Pilot-Aufbaus wurde auch eine Integration in das Sophos MDM System der Stadt Bern realisiert und mit einfachen Basis-Tests erfolgreich geprüft. Ausgedehnte Tests mit allen Funktionen wurden bewusst nicht durchgeführt, da die Funktionalität eines Mail- oder Kalender-Clients nichts mit MDM zu tun hat, sondern nur mit dem eingesetzten Server (OX) und Client (Handy). Bei der bereits in Kapitel 6.2.1 referenzierten OX-Installation sind kaum Synchronisationsprobleme bekannt, obwohl es dort über 7000 Berechtigte gibt und die Vielfalt der Endgeräte sehr gross ist: Es werden die privaten Handys genutzt (BYOD), es ist kein MDM-System im Einsatz.

6.2.6 Funktionstest

Als einfacher Funktionstest wurden Mails zwischen den verschieden Test-Usern ausgetauscht, darunter auch Einladungen zu Terminen.

6.3 Testdurchführung

Die Resultate der Plattform-Tests stützen sich auf direkte Erfahrungen mit einer produktiven Installation mit über 30'000 Mail-Konten. Die Test-Plattform wurde als Testmandant in die MDM-Infrastruktur soweit integriert, dass die wichtigsten Groupware-Funktionalitäten auch von Handys aus getestet werden konnten. Die Client-Tests wurden bewusst nur mit dem Web-Client von OX durchgeführt – schliesslich ist eine der Empfehlungen dieser Analyse, wo immer möglich auf Web-Applikationen zu setzen.

6.3.1 Testfälle / Ergebnisse

Hinweis: wie unter 3.5.3 erwähnt, wird im Folgenden die Fehler-Kategorie «Darstellungsmangel» im übertragenen Sinn als «kleiner Mangel» benutzt.

6.3.1.1 Plattform

Testfall Nr.	**Bezeichnung** Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	**Ergebnis / Bewertung**
TFC001	**Netzwerk**: Nach Netzunterbruch verbindet Client wieder (ohne Neustart, ohne Datenverlust) Es wurde nur der Web-Client getestet. Solange nicht auch der Browser neu gestartet wird, gibt es keinen Datenverlust.	Erfolgreich
TFC002	**Management**: Monitoring / Reporting / Web Management Monitoring/Reporting: Open exchange ist über weite Strecken mit "Munin"-Messpunkten instrumentiert. Mit einem Munin-Server lässt sich die Applikation detailliert überwachen. Für jeden Messpunkt stehen Zeitreihen zur Verfügung. Das Management wird fast ausschliesslich über die Kommandozeile erledigt.	Betriebserschwerend
TFC003/ TFC004	**Backup und Restore**: Single Item Recovery durch den User / Administrator Aus dem Papierkorb für den User, nachher nur noch durch den Administrator möglich Sämtliche Mails werden als Dateien abgelegt (und müssen auch so ins Backup). Alle weiteren Benutzendendaten (Kalender,	Erfolgreich

	Adressbücher, etc) sind in der mariaDB. Auch diese muss (als DB-Dump) ins Backup.	
TFC006	**Hochverfügbarkeit Client-Zugriff**: Client wechselt bei Serverausfall transparent auf zweiten Server Klassischer Load-Balancer für Web-Applikationen kann vorgeschaltet werden, ist aber nicht Teil des OX-Produkts.	Darstellungsproblem
TFC007	**Hochverfügbarkeit Datenbank**: System wechselt bei Ausfall eines Datenbank-Servers transparent auf anderen Wird durch die Implementation der Datenbank mit einem Galera-Cluster sichergestellt.	Erfolgreich
TFC008	**Georedundanz**: Ausfall eines ganzen RZs wird kompensiert Ist durch geeignete Verteilung der Knoten über die beiden RZs einfach sicherzustellen.	Erfolgreich
TFC010	**Lastverteilung** Am Frontend geschieht dies über DNS Round-Robin oder (besser, siehe TFC006 oben) mit einem vorgeschalteten Loadbalancer. Für den Mailstore stellt dies der Dovecot-Director sicher. Für die Lastverteilung beim Lesen in der Datenbank sorgt der Galera-Cluster. Geschrieben werden muss jede Mutation in jede Datenbank-Kopie.	Erfolgreich
TFC011	**Provisioning**: Werden im Active Directory neue User mit entsprechenden Attributen angelegt, sollen sie automatisch auch einen Mail-Account erhalten. Es konnte nicht auf unmittelbare Erfahrungen mit der Anbindung von Active Directory an OpenXchange zurückgegriffen werden. Die Vergleichsinstallation ist an ein openLDAP von UCS angebunden, das Provisioning wird von UCS zur Verfügung gestellt. OX bietet alle notwendigen Schnittstellen und auch Beispiel-Implementationen für das Provisioning aus Active Directory. Das Provisioning ist nicht Teil des Produkts, kann aber in wenigen Wochen auf die Bedürfnisse der Stadt Bern angepasst und eingesetzt werden.	Betriebserschwerend
TFC012 TFC013	**Kadenz Patchmanagement** „Major Releases“ werden jeweils mindestens 12 Monate supported, pro Jahr gibt es ca 2 „major releases“. Für einen „major release“ gibt es je nach Bedarf „minor releases“. Erscheint ein neuer „minor release“, wird der vorletzte „minor release“ noch 3 Monate supported. Es ist also mit 2-4 Upgrades pro Jahr zu rechnen. Diese können – bei entsprechender Architektur und entsprechendem Vorgehen – unterbruchsfrei vorgenommen werden.	Erfolgreich

TFC014	**Support/Pikett**: Normalerweise reicht Support zu normalen Bürozeiten. In Ausnahmefällen (z.B. Wahlen) ist aber ein Pikettdienst übers Wochenende notwendig Open Xchange bietet unter anderem 24x7 Support-Modelle an. Ob diese auch punktuell gebucht werden können, ist Verhandlungssache.	Keine Bewertung

6.3.1.2 MDM (TFC015)

Zusammen mit der Stadt Bern wurde die Pilotinstallation ins MDM-System integriert. Die Basis-Tests (Senden/Empfangen/Synchronisieren von einigen Mails und Terminen) haben funktioniert.

6.3.1.3 Client

Testfall Nr.	**Bezeichnung** Testfall Beschreibung, Hinweis zu Testdurchführung und -dokumenten	**Ergebnis / Bewertung**
TFC016 TFC017	Benutzende können eigene Mailbox an **andere selektiv berechtigen** Diese Funktionalität war bei der Stadt Bern nicht installiert/konfiguriert, das Ergebnis kommt aus der Vergleichsinstallation. Jeder «Folder» (also z.B. «INBOX») kann individuell berechtigt werden: Lesen, Lesen/Schreiben und Lesen/Schreiben/Löschen	Erfolgreich
TFC018	„**Send as**“ / „**Send on behalf**“ Ein Versenden unter anderem Namen ist nicht möglich, als Absender einer Mail gilt immer die Person, die am Web-Client angemeldet ist.	Betriebsverhindernd
TFC019	**Räume/Ressourcen verwalten** Diese Funktionalität war bei der Stadt Bern nicht installiert/konfiguriert, das Ergebnis kommt aus der Vergleichsinstallation. Ressourcen können (durch entsprechend Berechtigte) definiert werden. Ist eine Ressource zum Zeitpunkt der Einladung bereits belegt, kann die Einladung nicht abgeschickt werden. Dies funktioniert zwar nicht gleich wie bei Exchange, verhindert aber eine doppelte Belegung effektiv.	Erfolgreich
TFC020	**Unpersönliche Mailbox** Es wird ein separater Account angelegt (unpersoenlich@bern.ch) und die notwendigen Personen berechtigt. Wegen der Einschränkungen aus TFC018 können Mails nur im Namen dieser Mailbox verschickt werden, wenn auch mit diesem Account eingeloggt wird.	Betriebserschwerend
TFC021	**Synchronisation von Mobilen Devices** Siehe oben TFC015	Erfolgreich

TFC022	**Web Client** (analog owa.bern.ch) Vorhanden	Erfolgreich
TFC023	**Schnellbausteine / Textbausteine konkretisieren** gibt es im WebClient nicht	Betriebserschwerend
TFC024	**Serienmails aus Word (.html)** Es gibt keine Schnittstellen direkt aus Word oder anderen Office-Programmen. Dieses Problem kann gelöst werden, indem z.B. Outlook mit dem «Outlook Oxtender» oder spezialisierte Programme für Serienmails benutzt werden. Eventuell möglich ist eine Lösung mit Libreoffice (es gibt einen Modus für personalisierte (Papier-) Serienbriefe, es ist aber unklar ob dies auch gleich für den elektronischen Versand genutzt werden kann)	Betriebserschwerend
TFC025	**Adressbuch** (Organisationsstruktur/Persönlich) OX stellt die Kontakt-Information aller lokalen Email-Accounts zur Verfügung. Es können mehrere persönliche Adressbücher geführt und auch wieder mit anderen geteilt werden.	Darstellungsmangel
TFC026	**Aufgaben** (zuweisen/organisieren/Fälligkeit/Teilerledigungen) Ist möglich, aber nicht wie in Outlook.	Darstellungsmangel
TFC027	**Adressen** in anderen Office-Programmen verwenden Alle Adressen können als CSV oder als vCard exportiert werden	Erfolgreich
TFC028	**Erweiterte Regeln für den Posteingang bzw. Antworten** (nicht Abwesenheitsass, SIEVE) Open Xchange benutzt für die Mails Dovecot, Dovecot hat eine vollständige SIEVE-Implementation	Erfolgreich
TFC029	(bestehende) **Kategorien auf Mails, Tasks** etc. Es können lediglich Farben zugewiesen werden, es gibt ca 10 Farben (nicht erweiterbar).	Darstellungsmangel
TFC030	**Suchordner** (nach Kriterien) Kriterien je nach Suche (Mails, Kontakte) sehr begrenzt	Erfolgreich
TFC031	**Regeln** (neu anlegen und bestehende übernehmen (Migration)) Anlegen ist möglich. Bestehende können nur übernommen werden, wenn sie Serverseitig (SIEVE) implementiert sind.	Betriebsverhindernd
TFC032	**Wiedervorlagen** (vorbereitete Mailvorlagen vom Share) Identisch nur mit Outlook und Oxtender möglich. Ähnliche Funktionalität (zentrale Mailvorlagen) würde mit einer unpersönlichen Mailbox, welche einen Folder mit Mailvorlagen an alle berechtigt erreicht.	Erfolgreich
TFC033	**Ext. Daten übernehmen** (z.B. VCard) VCards können in ein eigenes Adressbuch importiert werden.	Erfolgreich

TFC034	**Spezialsuche** (Mehrere Kriterien, speicherbar) Nicht vorhanden.	Betriebsverhindernd
TFC035	**Rechtschreibung und Grammatik** Rechtschreibung vom Browser wird benutzt.	Erfolgreich
TFC036	**normal e-mail.dot** Nicht vorhanden, kann aber analog zu TFC032 gelöst werden.	Betriebsverhindernd
TFC037	**Mail Austausch über eine externes Netz** Im Testbetrieb nicht, ansonsten Ja	Erfolgreich
TFC037a	**Verschiedene Signaturen** Beim Versenden einer Mail soll man zwischen mehreren Signaturen wählen können.	Erfolgreich
TFC038	Die **Suche** in einer Mailbox muss **vergleichbar performant** sein	Nicht getestet
TFC039	**Einschränkung der Anzahl Empfänger pro E-Mail** Kann konfiguriert werden	Erfolgreich

6.4 Migrationszenario auf OSS Produkte

Sollte die Stadt Bern entscheiden, von Microsoft Exchange auf OX zu migrieren, müssen natürlich auch sämtliche bestehenden Mails, Kalendereinträge etc. von Exchange nach OX migriert werden. Im Folgenden werden einige wichtige Eckpunkte einer solchen Migration diskutiert.

Mengengerüst: Aktuell hat die Stadt Bern ca 4000 Mail-Accounts und einen Gesamtdatenbestand von ca 5TB.

Migrationsgeschwindigkeit: Bei einer bei einem anderen Kunden durchgeführten Migration konnte ein Durchsatz von ca 50GB/Stunde erreicht werden. Dieser Durchsatz ist natürlich von einer Vielzahl von Faktoren abhängig und erst definitiv bekannt, wenn das auf den echten Systemen getestet wurde. Wenn alles optimal laufen würde und die Zahlen so stimmen, würde das eine reine Migrationszeit von ca 100 Stunden ergeben. In der Praxis kann aber immer etwas schiefgehen, es muss deshalb eine grosszügige Reserve (Faktor 2) eingeplant werden.

Verfügbarkeit: Da es sich bei der angedachten Migration um zwei komplett verschiedene Systeme handelt, darf ein Postfach während der Migration nicht mutiert werden (keine neuen Mails, weder empfangend noch sendend). Es muss also während einer gewissen Zeit verhindert werden, dass Personen ihren Mail-Account benutzen. Auch müssen die Benutzenden wissen, bis wann sie das alte System benutzen dürfen und ab wann sie die neue Lösung benutzen können. Ein Unterbruch für eine Person darf wahrscheinlich auch am Wochenende/an Feiertagen nicht länger als 24 Stunden dauern, besser wäre wohl ein Unterbruch nur von 12 Stunden (z.B. Samstagabend 20:00 Uhr bis Sonntagmorgen 8:00 Uhr).

Parallelbetrieb: Aus der Kombination von Geschwindigkeit und Verfügbarkeit ist klar, dass nicht alle Mails auf einen Schlag migriert werden können, der Betrieb wäre zu lange unterbrochen. Selbst bei einer deutlichen Verbesserung wird es ohne Parallelbetrieb (ein Teil der Benutzenden ist noch auf der alten Lösung, ein Teil bereits auf der neuen Lösung) nicht gehen. Es muss also eine Architektur aufgebaut werden, welche es erlaubt, über mehrere Wochen die User in zwei verschiedenen Mailsystemen zu

führen. Mails von aussen müssen zuerst an einen „Verteil-Server“[15] geleitet werden. Auch müssen beide Mailsysteme so konfiguriert werden, dass sie Mails ausschliesslich via diesen Verteil-Server verschicken, auch wenn die Mails anscheinend intern sind.

Datenformate/Funktionalität: Email ist in diversen RFCs standardisiert, die Migration von Mails ist verlustlos möglich. Bei allen anderen Groupware-Funktionen (Kontakte, Termine, Tasks) geht die Standardisierung deutlich weniger weit. Migrationen in der Vergangenheit haben gezeigt, dass z.B. Kalendereinträge problemlos migriert werden, aber die Verbindung zu anderen Benutzenden leidet. Wenn also die einladende Person eine migrierte Einladung aktualisiert, werden die eingeladenen Personen nicht mehr informiert. Das liegt daran, dass MS Exchange die Personen nicht über die E-Mail-Adresse, sondern über eine interne Exchange-ID referenziert. Ob dies immer noch so ist oder ob die neueren Migrationstools damit besser umgehen können, müsste in der Praxis erprobt werden.

6.4.1 Erfüllung der Anforderungen

Wie die Tests ergeben haben, können die Anforderungen der meisten Anwendenden mit dem OX-Web-Client erfüllt werden.

Wirklich fehlen dürfte die Möglichkeit, eMails im Namen von anderen Personen zu verschicken, sei es versteckt oder offengelegt („send as“/„send on behalf of“).

Stellenweise vermisst würde sicher auch die Integration von Outlook mit den anderen Microsoft Office Produkten. Aber diese Art von Integration ist ohnehin von der Desktop-Architektur abhängig und muss auf längere Zeit durch eine Integration auf Ebene Web-Applikation abgelöst werden. OX geht diesen Weg bereits ein Stück weit: Es integriert einen Netzwerk-Drive und eine Office-Lösung innerhalb der Web-Applikation (nicht getestet bei der Stadt Bern).

Die konkrete Anwendung von Groupware im OX-Webclient unterscheidet sich von Outlook. Wie es um die Akzeptanz eines neuen Clients bei den Angestellten steht, wurde nicht untersucht. Es gibt zwar die Möglichkeit, mit einem Plugin („OXtender“) Outlook auf dem Desktop mit OX im Hintergrund zu benutzen, aber das funktioniert natürlich nur, solange der Client weiterhin Windows ist (und spart damit auch keine Lizenzen).

Wie genau die Anforderung „Serienbrief per E-Mail“ beim Einsatz von OX umgesetzt werden würde, müsste noch abgeklärt werden, sehr wahrscheinlich müsste ein zusätzliches Tool eingesetzt werden.

6.4.2 Auswirkungen auf den IT Betrieb

Wir nehmen an, dass der Personalbedarf bei einem Ersatz von Exchange durch OX eher etwas erhöht wird: Ein redundantes OX-System besteht aus relativ vielen und teilweise auch unterschiedlichen Komponenten. Das aktuelle Exchange-System hingegen wird aus sechs ähnlichen Systemen zusammengebaut. Die interne Komplexität ist ähnlich, da letztlich dieselben Aufgaben zu bewältigen sind, aber mit dieser kommt man als System-Administrator seltener in Berührung.

Das benötigte Know-how umfasst OX selbst, Datenbank-Cluster und Dovecot-Cluster.

Die Komplexität für die Benutzenden bleibt beim Umstieg von Exchange auf OX etwa dieselbe, trotzdem ist eine fakultative Schulung anzubieten.

Gemäss kurzen Recherchen würde eine auf OX basierte Groupware-Lösung auch von Sophos unterstützt: Die Anforderung an die Groupware ist lediglich, dass das EAS-Protokoll unterstützt wird.

Nicht untersucht wurde die weitere Integration in die Infrastruktur der Stadt Bern wie z.B. Call-Center, Fax-Lösung, Anzeige-Systeme für Sitzungszimmer mit Integration in den Exchange-Kalender, … Dort ist mit weiteren Migrationskosten zu rechnen.

---

[15] Dieser Server muss prüfen können, ob ein Account auf dem alten oder neuen System «zuhause» ist und dann die e-Mails entsprechend zustellen.

6.4.3 Vendor Lock-In

Der Vendor Lock-In: Das Produkt Exchange/Outlook setzt zwar über weite Strecken auf Internet-Standards, definiert aber an verschiedenen Stellen eigene Erweiterungen, die Konkurrenz-Systeme nicht oder nicht genau gleich umsetzen können. Selbst wenn eine Migration einigermassen verlustlos möglich wäre (nicht unterstützte Features könnten als "Kommentare" den alten Daten hinzugefügt werden), werden gewisse Benutzendenkreise lieb gewonnene Features – vornehmlich im Outlook-Client – in der neuen Umgebung vermissen.

Selbst wenn OX sämtliche Exchange/Outlook-Features unterstützen würde, wäre eine Altdaten-Migration in dieser Grössenordnung ein mehrmonatiges Projekt. Dies ergibt auch eine Art Lock-In: Wenn der Betrieb einer neuen Lösung nicht günstiger als der Betrieb der aktuellen Lösung, gibt es keinen «return on investment» und es muss schon sehr gute Argumente für eine neue Lösung geben. Zudem ist dieser «technische» Lock-In bei jeder Groupware-Lösung ähnlich.

6.5 Kostenvergleich

6.5.1 Szenario

OpenXchange Groupware anstatt MS Exchange

- Mengengerüst 2500 User
- Subscriptions und Support teilweise 24/7 gerechnet, bei Mailsystemen unumgänglich
  - 3 x MariaDB
  - 2 x HA Proxy
  - 2 x Dovecot/IMAP
  - 2 x Webmail/OX
- Subscriptions: 9 x RHEL (Cluster) / 3 x MariaDB (Galera)
- Subscriptions: 2'500 User für OX App Suite

6.5.2 Investitionen

- **Basisapplikation (Outlook)**: Nicht relevant, da Verwendung des Webclients gerechnet
- **Admin/Support-Schulung:**
  - Annahme: 3 Admins mit je 8 Tagen externer Schulung für den ganzen OX und Mailstack.
- **Engineering/Setup, Migration**: Der Aufbau einer OX-Mailumgebung, deren Integration in die Stadtberner Informatik (AD-Anbindung) und die Migration der Daten
- **Benutzendenschulung:**
  - Annahme: Es wird von einer umfassenden Schulung aller Anwendenden ausgegangen. Theoretisch liesse sich wohl mit einer guten Dokumentation vieles ohne Schulung machen lassen. Dies entspricht aber nicht der Philosophie der Stadt Bern, wo eher auf Schulung als auf selbstständige Einarbeitung gesetzt wird.
  - Es wird mit einem Aufwand von 2 Stunden pro User gerechnet.

Es wird angenommen, dass die Schulungen durch die Stadt Bern selber durchgeführt werden

Pilot C: Investitionen

		Zusätzliche Investitionen Aufbau OSS Plattform												
		Administratoren / Support Schulung			Engineering / Systemaufbau			Migration (Daten / Schnittstellen)			Benutzer-schulung			Total
Bereich		int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT 4)			0			0			0			0	0
	Basisapplikationen (KAT 1 und KAT 2)			0			0			0			0	0
	Office Suite (KAT 1)			0			0			0			0	0
	Betriebssystem			0			0			0			0	0
	Hardware			0			0			0			0	0
Netzwerk	WAN			0			0			0			0	0
	LAN			0			0			0			0	0
Data Center	WEB Applikationen	24	16	6'680			0			0	5'322	16	774'890	781'570
	Virtualisierungs-plattform			0			0			0			0	0
	SW Deployment			0			0			0			0	0
	Zentrale Applikationen	576	160	115'520	600	900	267'000	1'200	900	354'000			0	736'520
	Datenbank			0			0			0			0	0
	HW / Server / OS			0			0			0			0	0
	RZ Raum/Strom/Klima			0			0			0			0	0
Total				122'200			267'000			354'000			774'890	1'518'090

6.5.3 Betriebskosten

- **Subscriptions**: Standard für RHEL und MariaDB, Premium für OX
  - RHEL (Cluster): 9 x 760 CHF = 6'840 / Jahr
  - MariaDB Galera: 3 x 7500 CHF = 22'500 Jahr (nicht zwingend notwendig)
  - OX App Suite: (2500 User x 30 CHF),
    - plus Aufwände / SLA mit einem externen Spezialisten
      - SLA Fixkosten: 15'000 CHF / Jahr
      - Aufwände für Support und Störungsbehebung: 36'000 CHF / Jahr
- **Interne Betriebsleistungen**:
  - Annahme: Die Aufwände für Support und Betrieb bewegen sich in etwa in derselben Grössenordnung wie die Aufwände für den Betrieb von MS Exchange

Pilot C: Betriebskosten

		Reduktion bisheriger Betriebsaufwand / Jahr						Zusätzlicher Betriebsaufwand OSS /				Vergleich
		Lizenzen		Admin / Support			Total	Subscriptions	Admin / Support		Total	
Bereich		Anzahl	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]	ext.	int. [h]	[CHF]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT 4)					0	0			0	0	0
	Basisapplikationen (KAT 1 und KAT 2)					0	0			0	0	0
	Office Suite (KAT 1)					0	0			0	0	0
	Betriebssystem					0	0			0	0	0
	Hardware					0	0			0	0	0
Netzwerk	WAN					0	0			0	0	0
	LAN					0	0			0	0	0
Data Center	WEB Applikationen					0	0			0	0	0
	Virtualisierungs-plattform					0	0			0	0	0
	SW Deployment					0	0			0	0	0
	Zentrale Applikationen	6	-3'650	-500		-72'500	-76'150	134'000	500	72'500	206'500	130'350
	Datenbank					0	0	22'500		0	22'500	22'500
	HW / Server / OS					0	0	6'840		0	6'840	6'840
	RZ Raum/Strom/Klima					0	0			0	0	0
Total			-3'650			-72'500	-76'150	163'340		72'500	235'840	159'690

6.6 Zusammenfassung

6.6.1 Ergebnisse

Der Pilot C hat gezeigt, dass eine OSS Groupware Lösung aufgebaut und mit der notwendigen Redundanz betrieben werden kann. Die meisten benötigten Funktionen sind implementiert. Als betriebsverhindernde Einschränkung wird die Tatsache gewertet, dass unter anderem Funktionen wie z.B. "Send on behalf" nicht verfübar sind.

6.6.2 Chancen

Der Einsatz von OSS anstelle von proprietärer Software bietet im Pilotprojekt C folgende Chancen:

- Lösen der Abhängigkeit von marktdominanten Herstellern
- Nutzen der neu entstehenden Wettbewerbssitution

6.6.3 Risiken

Der Einsatz von OSS anstelle von proprietärer Software birgt im Pilotprojekt C folgende Risiken:

- Unzufriedenheit der Benutzenden, welche OSS Produkte einsetzen werden, wegen einer fehlenden Funktionalität bzw. Darstellungsmängel
- Integrationen mit Sitzungszimmer, Call Center funktionieren mit grösster Wahrscheinlichkeit. Der Support durch die Hersteller ist jedoch nicht gewährleistet.

6.6.4 Finanzen

- Einsparung von Microsoft Windows Lizenzen: TBD
- Investitionen für den OSS Plattform Aufbau und OpeneXchange

6.6.5 Empfehlung

- Von der Kern-Funktionalität und Stabilität alleine her wäre OpenXchange als OSS Lösung für Groupware eine durchaus gangbare Variante. Trotzdem muss zur Zeit von einem Wechsel abgeraten werden. Der Support für integrierte Umsysteme (MDM, Call-Center, Serienbriefe etc.) ist nicht gewährleistet. Auch ist unklar, ob alle Anwendenden mit den fehlenden Funktionalitäten (z.B. "Send on behalf") leben können.
- Mit einem Vorprojekt die kritischen Punkte (Support Umsysteme, Benutzer-Akzeptanz, Security) abklären
- Fehlenden Funktionalitäten können von entsprechenden Partnern im Auftrag entwickelt werden

6.6.6 Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Es fehlen wichtige Funktionen (z.B. «im Auftrag versenden») und Desktop-Integrationen.
Sicherstellen des stabilen Informatikbetriebs	Die Kernfunktionen sind verfügbar, aber es gibt keinen Support für serverseitige Integrationen.
Wirtschaftlichkeit	Eine Migration ist aufwändig, die Kosten für den Betrieb sind vergleichbar.
Abhängigkeit von dominanten Marktteilnehmenden	Sämtliche Daten werden in offenen Formaten gespeichert und sind über offene Schnittstellen zugreifbar.

7 Pilotprojekt D: Client Virtualisierung

7.1 Anforderungsdefinition

Bei der Virtualisierung geht es darum, mehrere "Computer" auf einer physischen Maschine laufen zu lassen. Die Vorteile sind:

- in der Regel können die Ressourcen besser genutzt werden (mehr Services mit weniger Hardware)
- (praktisch) unterbruchsfreier Betrieb

Der Betrieb von virtuellen Maschinen ist eine stabile, etablierte Technik. Die Software, die es ermöglicht, einzelne virtuelle Maschinen ("Guests") auf einer physischen Maschine ("Host") zu betreiben, heisst "Hypervisor". Es gibt verschiedene Hypervisoren für die x86-Architektur (vmware, Hyper-V, KVM, Xen, …). Diese haben ihre individuellen Vor- und Nachteile, sind heute aber alle stabil und verlässlich. Der Hypervisor ist die minimal notwendige Basis für den Betrieb von virtuellen Maschinen. Vereinfacht gesagt, kann man als "Administrator" mit dem Hypervisor bereits virtuelle Maschinen erzeugen und laufen lassen.

Für den Einsatz in Unternehmen muss die Plattform aber den sicheren Betrieb auch für mehrere User erlauben, zum Beispiel muss der Verbrauch von Ressourcen (CPU, RAM, Storage) pro Abteilung limitiert werden können, nicht jede VM darf von jeder Person neu gestartet werden, usw. Beispiele dafür sind vSphere (mit vmware als Hypervisor), Hyper-V, RHV (mit KVM) oder Citrix Xen-Server (mit Xen). Auf dieser Stufe werden die Unterschiede bereits grösser.

Ein weiterer Gesichtspunkt ist der Einsatzzweck der virtuellen Maschinen: Bei der **Server-Virtualisierung** geht es für eine VM im Wesentlichen darum, "Aufträge" via Netzwerk entgegenzunehmen, unter optimalem Einsatz von CPU, RAM und Disk zu bearbeiten und die Antworten ebenfalls via Netzwerk zurückzuliefern. Benutzende "sehen" also den virtualisierten Server gleich wie einen physischen, nämlich lediglich über das Netzwerk. Bei der **Client-Virtualisierung** muss für die Benutzenden auch eine Tastatur, eine Maus und ein Bildschirm zur Verfügung gestellt werden. Auch Audio (Mikrophon/Lautsprecher) und generell USB-Geräte sind ein Thema. Das ruckelfreie Abspielen eines Films in hoher Auflösung ist immer noch eine Herausforderung, Filme bearbeiten und schneiden erst recht. Auch wenn Filme schauen und produzieren kaum zum Aufgabenkatalog von städtischen Angestellten gehört – schon bei IP-Telefonie stören Aussetzer extrem.

Citrix unterstützt nicht nur den Betrieb eines kompletten Desktops über das Netzwerk, sondern auch das Ausführen von einzelnen Applikationen übers Netzwerk: **Applikations-Virtualisierung**. Die Applikationen können aus dem Standard-Menü aufgerufen werden und öffnen sich auf dem Desktop des Benutzenden als wären sie lokal installiert. Der Start dauert etwas länger als normal und man sieht den Citrix-Login – dank SSO muss aber kein Passwort mehr eingegeben werden. Diese Technik vereinfacht den Unterhalt der Desktop-PCs (die Applikation muss nicht mehr lokal installiert werden) und spart Ressourcen in der Virtualisierung (es muss nicht für jede Session eine separate VM mit Betriebssystem betrieben werden).

7.2 Umsetzung

7.2.1 Lösungsansatz

Als Produkt wurde die Red Hat Virtualization (RHV) gewählt. Das Produkt hat sich als zuverlässiges System etabliert. RHV kann (wie auch Citrix und wmware) sowohl Windows- als auch Linux virtualisieren.

Zu Beginn des Projekts bot keine verbreitete OSS-Virtualisierungslösung speziellen Support für Client-Virtualisierung – auch RHV nicht. Insbesondere fehlt Support für:

- Applikations-Virtualisierung
- SSO
- optimierte Verwaltung des Windows-Profils

Trotzdem wurde der Projektauftrag soweit möglich umgesetzt:

- Tests wurden mit dem virtualisierten OSS-Client aus Pilot A/B durchgeführt. Dieser ist identisch für alle User, nur der Login entscheidet, welche Applikationen und Daten zur Verfügung stehen.
- Eine Virtualisierung von Windows-Clients wurde nicht untersucht, das Handling der Benutzenden-Profile müsste mit «klassischen» Mitteln gemacht werden. Dies bedeutet unter anderem, dass für dieselbe Anzahl aktive User mehr Ressourcen auf den zentralen Hosts bereitgestellt werden müssten.

7.2.2 Aufbau der Infrastruktur

Die Stadt Bern hat folgende Komponenten bereitgestellt:

- VM für RHV Management Software (1 CPU, 16GB RAM, 60GB Disk)
- Hardware für zwei Hypervisoren (je 24 CPUs, 144GB bzw. 216GB RAM, je 120GB Disk
- Netzwerkkonfiguration
- Storage-Export (500GB NFS) ab NetApp für die Ablage der virtuellen Maschinen

Der Einfachheit halber haben alle drei Hosts dasselbe Passwort. Der User via SSH ist root, für die Management-Konsole ist der Name admin zu verwenden.

7.2.3 Installation RedHat Virtualization Manager

Auf der von der Stadt Bern bereitgestellten VM wurde ein RedHat Enterprise Linux Server 7.4 installiert. Die Installation wurde mit dem Minimal-Profil gemacht.

7.2.4 Installation einer VM

Die Installation einer VM in RHV ist ähnlich wie in anderen Umgebungen: Es werden zuerst die physichen Parameter der neuen VM (Anzahl CPUs, Grösse RAM) und der Storage (z.B. eine virtuelle Disk) definiert. Anschliessend kann das Betriebssystem installiert werden.

Soll zum Beispiel der in Pilot A/B erarbeitete Client installiert werden, muss lediglich die MAC-Adresse der erzeugten VM in Foreman eingetragen werden. Dann kann der virtuelle Client gestartet werden und er wird sich selber installieren.

Es gibt in RHV auch einen Template-Mechanismus. Dieser umfasst aber nur die Parameter zur Erzeugung einer VM und nicht, wie man für einen idealen VDI-Betrieb erwarten würde, das komplette Disk-Image. Es werden also auch nicht dynamisch neue VMs erzeugt, sondern es müssen im Voraus sämtliche VMs bereitgestellt werden.

7.2.5 Bereitstellen der Test-Daten

Es gibt keine spezifischen Test-Daten für dieses Pilotprojekt.

7.2.6 Anbindung der Schnittstellen

RHV bietet gegen aussen zwei Benutzenden-Schnittstellen an: Das Administrations-Portal und das User-Portal. Im User-Portal sehen die Benutzenden nach dem Logon nur diejenigen VMs, die Ihnen gehören. Für den vorliegenden Fall "Client-Virtualisierung" erteilt man den Benutzenden keine Berechtigung, neue VMs zu erstellen, diese werden ausschliesslich von Administratoren erstellt.

7.2.7 Konfigurationen

Die einfachste Variante, den RHV-Manager (mit dem Administrations- und User-Portal) redundant vorzuhalten, ist diesen als "self hosted engine" zu betreiben. In diesem Fall ist der Manager eine VM auf RHV mit speziellen high availability Einstellungen. Insbesondere kümmert sich RHV darum, dass eine

aktuelle Kopie des RAM-Inhalts der VM auf mindestens einem anderen host permanent vorgehalten und aktualisiert wird. Dies ist mittlerweile die empfohlene Konfiguration.

7.2.8 Funktionstest

Ein Basis-Funktionstest besteht darin, eine VM aufzubauen und zu benutzen. Dies wurde mit den Testfällen unten (siehe 7.3.1) mehrfach gemacht und musste deshalb nicht separat getestet werden.

7.3 Testdurchführung

Die Testfälle wurden von der Stadt Bern definiert und wenn möglich durchgeführt. Dort wo die Durchführung nicht möglich/nicht sinnvoll war, wird dies entsprechend kommentiert.

7.3.1 Testfälle

Die Nummerierung der Testfälle ermöglicht die Zuordnung der Testfälle zu den Testprotokollen. Gewisse Testfälle wurden nach dem ersten Entwurf zusammengefasst oder fallen gelassen. Deshalb gibt es in der Nummerierung einige Lücken.

Die Resultate lassen sich wie folgt zusammenfassen:

- Die technische Basis der Linux-Virtualisierung ist erprobt und stabil
- Der Betrieb von Windows-VMs wird von RedHat offiziell unterstützt[16]
- Gesamthaft ist RHV nicht geeignet, den Platz von Citrix bei der Stadt Bern einzunehmen: Zentrale Anforderungen an eine Client-Virtualisierungslösung sind nicht umsetzbar. Speziell zu nennen sind:
    - RHV „Templates“ umfassen nur die Parametrisierung der virtuellen Hardware (Anzahl virtuelle CPUs, Grösse von virtuellem RAM und virtueller Disk), aber nicht den Inhalt der Harddisk. Deshalb können sie nicht dafür verwendet werden, ein einziges „Image“ für 1500 User bereitzustellen.
    - Es ist für eine VM in RHV nicht möglich festzustellen, ob sie „von innen“ (vom Intranet) oder „von aussen“ (vom Internet) her angesteuert wird
    - In einer einfachen Installation gibt es kein SSO – das heisst ein Benutzer muss sich zuerst bei RHV anmelden, dann nochmal am Windows-Logon. Ob und wenn ja wie weit sich dies optimieren lässt, müsste in einem separaten Projekt geklärt werden. Siehe dazu auch TFD022 in Abschnitt 7.3.1.18.

7.3.1.1 TFD001 – IP-Adressierung

Frage: Wie werden mehr als 1500 VMs adressiert?

7.3.1.1.1 Durchführung

Keine

7.3.1.1.2 Ergebnis

RHV stellt virtualisierte Netzwerke ausschliesslich auf Layer 2 zur Verfügung. DHCP kann extern von einer bestehenden DHCP-Lösung bezogen werden. Wenn nötig, kann auch eine VM erstellt werden, welche einen eigenen DHCP-Dienst zur Verfügung stellt. Damit können auf Layer 3 die IP-Netze nach Bedarf dimensioniert werden (1 grosses oder mehrere kleine Subnetze).

[16] https://access.redhat.com/articles/973163

7.3.1.2 TFD002 – IP Ports

Das SPICE Protokoll, welches für die Übertragung von Bildschirm-Inhalten, Tastatur und Maus-Inputs etc. verantwortlich ist, benutzt die TCP ports 5634 – 6166[17].

7.3.1.3 TFD003 – Live Migration während Benutzendensession

Vorgabe: "Durchführen einer Life Migration während die Benutzendensessions laufen"

7.3.1.3.1 Durchführung

- Im RHV User-Portal einloggen
- Eine VM starten und die Konsole öffnen
- Login in das Administrationsportal als Administrator
- Wechseln auf den Tab "Virtuelle Maschinen"
- Rechtsklick auf der gewünschten VM
- Migrieren auswählen
- Automatisch oder den gewünschten Host auswählen
- Während der Migration die VM benutzen

7.3.1.3.2 Ergebnis

Die Live-Migration ist erfolgreich, die VM läuft nach der Migration auf dem zweiten Host. Benutzende merken davon nichts.

7.3.1.4 TFD004 – Live-Migration Host für Update

Vorgabe: "Leerräumen“ eines physischen Hosts (z.B. für Upgrades)

7.3.1.4.1 Durchführung

- Login in das Administrationsportal als Administrator
- Wechseln auf den Tab "Hosts"
- Rechtsklick auf den gewünschten Host, "Management", "Wartung"
- Der Host wird in den Wartungsmodus gesetzt, dabei werden alle virtuellen Maschinen auf andere verfügbare Hosts migriert

7.3.1.4.2 Ergebnis

Der Test konnte erfolgreich durchgeführt werden. Der Host ist in den Wartungsmodus versetzt, alle laufenden VMs wurden auf den zweiten Host verschoben. Updates könnten nun installiert werden.

7.3.1.5 TFD005 – Monitoring Systemressourcen

Vorgabe: "Monitoring der Systemressourcen (inkl. History)"

7.3.1.5.1 Durchführung

Das bereits vorhandene Monitoring wurde angetestet.

[17] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Virtualization/3.1/html/Administration_Guide/Virtualization_Host_Firewall_Requirements1.html

7.3.1.5.2 Testergebnis

Ein minimales Monitoring ist in RHV bereits integriert. Das Ziel ist aber, dass RHV in ein bestehendes Monitoring-Tool integriert wird.

Die System-Überwachung kann via bestehendem Tool (SCOM) erledigt werden. Um Daten aus dem RHV-Manager auszulesen, existiert eine API. Die Dokumentation der API ist öffentlich verfügbar[18].

Dank der API ist es möglich die Daten auszuwerten und in eine Datenbank zu schreiben. Ein Beispiel für ein Plugin für nagios ist auf github zu finden[19]. Eine Anpassung für SCOM könnte in wenigen Tagen umgesetzt werden.

7.3.1.6 TFD006 – Alarmierung Systemressourcen

Vorgabe: "Alarmierung bei Überschreiten von "thresholds“"

7.3.1.6.1 Durchführung

Es wurde abgeklärt, welche Möglichkeiten für Mail-Eskalation bei RHV bereits vorhanden sind.

7.3.1.6.2 Testergebnis

In RHV ist eine Möglichkeit integriert, die es bei entsprechender Konfiguration ermöglicht, Emails bei Events zu versenden[20].

Emails können für diverse Events konfiguriert werden (Liste nicht abschliessend):

- Freier Arbeitsspeicher ist knapp
- Host ist erreichbar
- Netzwerkauslastung ist hoch
- Hohe CPU Auslastung
- VM antwortet nicht
- Speicherplatz ist knapp

7.3.1.7 TFD007 – Integration SCOM (Betriebserschwerend)

Vorgabe: Ist die Integration in SCOM Monitoring möglich?

7.3.1.7.1 Durchführung

Es wurde abgeklärt, welche Möglichkeiten zur Hardware-Überwachung der physischen Hosts mit SCOM bestehen.

7.3.1.7.2 Testergebnis

Es ist möglich, SCOM auf den Servern zu installieren. Der Support ist durch RedHat aber nicht gewährleistet[21].

---

[18] https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.1/pdf/rest_api_guide/Red_Hat_Virtualization-4.1-REST_API_Guide-en-US.pdf

[19] https://github.com/ovido/check_rhev3/blob/master/plugin-dir/check_rhev3.pl

[20] https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.1/pdf/administration_guide/Red_Hat_Virtualization-4.1-Administration_Guide-en-US.pdf

[21] https://access.redhat.com/solutions/3457751

Bei den Hostsystemen ist zu beachten, dass die manuell installierten Pakete nach einem Update gelöscht werden und wieder installiert werden müssen. Auf dem Manager werden installierte Pakete bei einem Upgrade aktualisiert, dort ist dies nicht nötig.

7.3.1.8 TFD008 – Ressourcenbedarf (Betriebserschwerend)

Vorgabe: Wieviele Ressourcen (RAM/CPU/Disk) würde eine Lösung basierend auf RHV für 1500 User benötigen?

7.3.1.8.1 Durchführung

Es wurden 20 virtuelle (Linux-) Clients parallel auf einem physischen Host gestartet. Jeder Client hat 8GB RAM erhalten. Ein zweiter Lauf mit "Memory Ballooning" wurde ebenfalls durchgeführt. Bei "Memory Ballooning" wird für RAM ein Minimum garantiert (hier: 4GB), bei Bedarf gibt es (wenn noch verfügbar) mehr – bis zum konfigurierten Maximum (hier: 8GB).

In beiden Fällen wurden die verwendeten Ressourcen direkt auf dem physischen Host überprüft

7.3.1.8.2 Testergebnis

Tests mit 20 Clients, **RAM**-Verbrauch auf physischem Host:

- mit Memory-Ballooning: 22 GB
- ohne Memory-Ballooning: 22 GB

Die gemessenen 22GB entsprechen lediglich 1.1GB RAM pro Client-VM. Dies ist deutlich weniger, als zu erwarten wäre (4 bzw 8GB pro Client-VM). Offensichtlich wird im Betriebssystem des physischen Hosts RAM erst alloziert, wenn es von den VMs tatsächlich benutzt wird (unabhängig vom Memory-Ballooning).

Mit diesen 22GB für 20 VMs würden total lediglich 1650 GB für 1500 Clients belegt. Das ist zwar ein sehr gutes Resultat, aber letztlich nur als **untere Grenze** brauchbar – wenn alle Clients gestartet sind, aber niemand darauf arbeitet. Eine realistische Messung war im gegebenen Rahmen zu aufwändig und leider nicht machbar.

Die **obere Grenze** für den RAM-Bedarf lässt sich aber einfach ausrechnen:

4 GB – 8 GB pro Client-VM: 6TB – 12TB RAM

Bei den **CPU-Cores** kann davon ausgegangen werden, dass bei gleicher Arbeitslast eine ähnliche Anzahl physischer Cores wie jetzt notwendig ist, um die gesamte Last zu tragen. Wegen der deutlich grösseren Anzahl VMs (eine VM pro Arbeitsplatz) im Vergleich zu heute (mehrere User teilen sich eine VM) ist allerdings mit tendenziell höherem CPU-Bedarf zu rechnen.

Aktuell benötigt ein Linux-Client ca 60GB **Harddisk**. Extrapoliert auf 1500 Clients ergibt das total 90TB. Je nach Speicherlösung wird aber nur ein Bruchteil davon tatsächlich auf physischen Speichermedien benötigt (zum Beispiel eine Netapp mit aktivierter Deduplikation).

7.3.1.9 TFD010 – Netzwerkverlust

Vorgabe: Ein physischer Hosts kann vom Netzwerk getrennt werden. Alle betroffenen VMs müssen auf einem anderen Host neu gestartet werden.

7.3.1.9.1 Durchführung

- Sicherstellen dass mindestens 2 Hosts verfügbar sind
- Mittels SSH auf dem einen Host einloggen
- systemctl stop network eintippen, um das Netzwerk auszuschalten. Die ssh-Verbindung wird dadurch sofort unterbrochen.
- In den Logs beobachten, dass RHV bemerkt dass der Node nicht mehr erreichbar ist

- RHV startet die VMs auf dem zweiten Host neu.

7.3.1.9.2 Testergebnis

Der Test war erfolgreich. Nachdem RHV bemerkt hat, dass der Host nicht mehr erreichbar ist, wurden alle Clients auf den zweiten Server migriert und dort neu gestartet. Für den User gab es dabei einen Unterbruch, da es eine gewisse Zeit dauert, die VMs neu zu starten.

7.3.1.10 TFD011 – Trennen eines Brokers

7.3.1.10.1 Durchführung

Die Pilotinstallation wurde mit einem externen Management Node erstellt. In dieser Konfiguration gibt es keinen Failover für das Benutzenden-Frontend. In neueren Versionen von RHV wird der Management Node standardmässig «self hosted» (d.h. als VM innerhalb von RHV) installiert. In dieser Konfiguration funktionieren natürlich alle Failovermechanismen von RHV auch für den Management Node.

7.3.1.10.2 Ergebnis

Geht (aber nicht getestet).

7.3.1.11 TFD012 – Verteilung über zwei RZ

7.3.1.11.1 Durchführung

Es wurde im Projekt beschlossen, der Einfachheit halber die Systeme nicht in zwei RZs aufzubauen.

7.3.1.11.2 Ergebnis

Kann analog zur jetzigen Lösung (dieselben VLANs in beiden RZs) implementiert werden.

7.3.1.12 TFD013 – Rolling Upgrade

"Rolling Upgrade“ muss möglich sein.

7.3.1.12.1 Durchführung

- Wenn update verfügbar, RHV Manager updaten
- Einen Host in den Maintenance-Mode versetzen
- Via Web-UI den Host updaten
- Nach Installation den Host wieder aktivieren
- Ab Schritt 2 für alle Nodes wiederholen

7.3.1.12.2 Testergebnis

Rolling-Upgrade ist möglich. Wird bei einer ähnlichen Installation schon seit Version 3.5 für jeden Upgrade so umgesetzt.

7.3.1.13 TFD014 – Aufwand Rolling Upgrade

Aufwand für einen Rolling Upgrade (Automatisierungsgrad)

7.3.1.13.1 Durchführung

Auf der Labor-Umgebung einen Upgrade durchzuführen und den Aufwand dafür zu messen, erschien uns nicht sinnvoll. Ein Erfahrungsbericht aus der Praxis ist nützlicher.

7.3.1.13.2 Testergebnis

Für ein Setup mit 6 Hosts und ca. 150 VMs wurden bei Adfinis-SyGroup AG jeweils ca. 2 Tage benötigt. Bei deutlich grösseren Umgebungen ist damit zu rechnen, dass dies effizienter wird, pro physischen Host wäre dann noch mit ca 2h pro physischem Host zu rechnen.

7.3.1.14 TFD015 – Einspielen von Patches auf VMs (betriebserschwerend)

7.3.1.14.1 Durchführung

Keine Durchführung

7.3.1.14.2 Ergebnis

Da bei einem OSS-Client für jede Person eine eigene VM bereitgestellt wird, genügt das Patching durch ansible (wie in Pilot A Kapitel 4.2.4.6 beschrieben). Allerdings müssten bei einem Setup mit einer virtuellen Maschine pro Session (siehe Kapitel 7.2.1) deutlich mehr virtuelle Maschinen aktualisiert werden. Dies ist zwar automatisiert, verbraucht aber mehr Ressourcen.

7.3.1.15 TFD016 – Aufteilung VMs auf physische Hosts

7.3.1.15.1 Durchführung

Es wurde kein Test durchgeführt.

7.3.1.15.2 Ergebnis

Gemäss einer älteren, aber grösstenteils immer noch zutreffenden Dokumentation[22] von oVirt (oVirt ist die technische Basis von RHV) kann die Zuordnung der VMs zu den jeweiligen Hosts über viele verschiedene Parameter beeinflusst werden.

Im einfachsten Fall werden einfach die VMs gezählt und möglichst gleich viele pro physischen Host gestartet.

7.3.1.16 TFD019 – Copy/Paste von "innen" nach "aussen"

Können Bildschirminhalte zwischen Programmen in der Virtualisierungs-Session und solchen ausserhalb ausgetauscht werden.

7.3.1.16.1 Durchführung

Wurde getestet.

7.3.1.16.2 Ergebnis

Funktioniert. Erschwerend wirkt oft, dass ein Linux-Desktop mehr als einen Copy/Paste Buffer hat und es nicht immer offensichtlich ist, welcher gerade benutzt wird.

7.3.1.17 TFD020 – Persönliche Einstellungen User

Wie werden die persönlichen Einstellungen der User nach einem Logout behalten?

7.3.1.17.1 Durchführung

Bei einem klassischen Desktop-PC werden die persönlichen Einstellungen von Benutzenden auf der lokalen Harddisk abgespeichert. Bei Windows ist das primär ein Teil der Registry, es können aber auch

[22] https://ovirt.org/develop/release-management/features/sla/scheduler-policies.html

("versteckte") Konfigurations-Dateien im Heimverzeichnis sein. Bei Linux gibt es ausschliesslich «versteckte» Konfigurations-Dateien im Heimverzeichnis.

Es wurden keine konkreten Tests durchgeführt, da sich die (zum grossen Teil) negativen Resultate schon alleine aus der Dokumentation ablesen lassen.

7.3.1.17.2 Testergebnis

In der jetzigen Implementation mit Citrix erhalten die Benutzenden bei jeder neuen Verbindung eine "neutrale" VM, welche neu aus einem generischen Image erstellt wird. In so einem Fall ist der benutzendenspezifische Teil der Registry leer und wird unter Citrix durch den "Citrix Profile Manager" aus dem Stand von der letzten Sitzung wiederhergestellt.

Da bei RHV für jede Session eine eigene VM bereitgestellt wird, ist zwar der Bedarf an Speicherplatz auf Disk viel grösser als bei Citrix. Anstelle des Profile Managers stellt das eigene Heimverzeichnis die eigenen Konfigurationen zur Verfügung (siehe 4.2.3).

7.3.1.18 TFD022 – SSO

"Weitergabe von Username / Passwort an mehrere Fachapplikationen gleichzeitig (Kerberos)".

RHV fällt in diesem Testfall (in seiner ursprünglichen Form) ohne weitere Prüfung durch, da RHV die Virtualisierung von einzelnen Applikationen gar nicht unterstützt. Wird die Frage auf den ganzen Desktop übertragen, heisst das (abgemildert): "Können Anwendende von ihrem Desktop einen virtualisierten Client starten und bedienen, ohne ein weiteres Mal ihr Passwort eingeben zu müssen?"

7.3.1.18.1 Durchführung

Selbst in der abgemilderten Form wäre die praktische Durchführung nur nach aufwendigen Engineering-Arbeiten möglich. Aus Benutzendensicht passiert (im Pilotbetrieb) aktuell folgendes:

1. Die Benutzende loggt sich lokal auf ihrem lokalen Linux-Client (aus Pilot A/B) mit Username und Passwort ein.
2. Sie öffnet im Browser das Admin-Portal von RHV und meldet sich dort (wieder mit Username und Passwort) an.
3. Im Admin-Portal startet sie "ihren" remote Linux-Client und meldet sich ein drittes Mal an.

Aus technischer Sicht muss für eine befriedigende SSO-Lösung also sowohl die Anmeldung 2 am Admin-Portal als auch die Anmeldung 3 am remote Client ohne Eingabe von Passwort funktionieren. Weiter ist die Frage erst dann vollständig beantwortet, wenn auch getestet wird, wenn der lokale und/oder der remote Client durch einen Windows-Client ersetzt werden.

Die diversen zur vollständigen Beantwortung der Frage notwendigen Konfigurationen konnten aber aufgrund der verfügbaren Zeit nicht alle entwickelt und aufgebaut werden. Auch im Hinblick darauf, dass RHV wegen diverser anderer Testfälle als "betriebsverhindernd" eingestuft werden muss, wurde auf diesen Test verzichtet.

7.3.1.18.2 Testergebnis

Single Sign On ist eine zentrale Architektur-Entscheidung für eine Organisation. In der Stadt Bern ist dies zur Zeit Kerberos (Microsoft Active Directory).

Eine der oben beschriebenen Kombinationen von Clients und Virtualisierung kann als getestet gewertet werden:

- Lokaler Client: Linux
- Virtualisierung: Xen
- Remote Client: Windows

Diese Kombination entspricht der Situation auf über der Hälfte aller physischen Workstations: Die Stadt Bern setzt dort Thin-Clients mit einem Linux-Betriebssystem ein.

Die jetzige Pilot-Installation (lokal und remote Linux-Client, RHV als Virtualisierung) funktioniert, aber es gibt kein SSO (Passwort muss dreimal eingegeben werden). Anscheinend wird erst seit kurzem daran gearbeitet[23].

7.3.1.19 TFD023 – Zuweisung Fachapplikationen

Kann sichergestellt werden, dass Benutzende nur auf die virtualisierten (Kat-3) Applikationen Zugriff haben, für die sie berechtigt sind (zB über eine AD-Gruppe)

7.3.1.19.1 Durchführung

Es wurde kein Test durchgeführt.

Bei einem individuellen Linux-Client pro Person können die ansible-scripts (Abschnitt 4.2.4.6) so angepasst werden, dass nur die Applikationen installiert/aktualisiert werden, auf die die Person Zugriff hat.

7.3.1.19.2 Testergebnis

Ist machbar.

7.3.1.20 TFD024 – lokale Applikationen im Fall von Remote Zugriff

Handling von lokal installierten Applikationen im Fall von Remote Zugriff

7.3.1.20.1 Durchführung

Es wurde kein Test durchgeführt.

7.3.1.20.2 Ergebnis

Es gibt zur Zeit keine Möglichkeit, innerhalb einer RHV-VM zu prüfen, ob der Login von innen (portalprod.bgov.ch) oder von aussen (portal.bern.ch) erfolgt. Deshalb kann hier kein spezielles Handling implementiert werden.

7.3.1.21 TFD025 – Einspielen von updates

Wie werden Upgrades eingespielt?

7.3.1.21.1 Durchführung

Es wurde kein expliziter Test durchgeführt, aber der Mechanismus mit ansible Scripts funktioniert sowohl auf den Test-Rechnern der Stadt Bern als auch – im produktiven Einsatz – bei einem anderen Kunden.

7.3.1.21.2 Ergebnis

Geht problemlos, siehe Abschnitt 4.2.4.6.

7.3.1.22 TFD026 – Schnittstellen

Die Stadt Bern setzt verschiedene USB-Geräte ein, die auch auf einer virtualisierten Umgebung funktionieren müssen. Dazu gehören:

- Smartcard für SwissID

[23] https://bugzilla.redhat.com/show_bug.cgi?id=884653

- Belegleser für Einzahlungsscheine (SAP)
- DVD (lesend) und Smartphones (lesend)

Aus Sicherheitsgründen dürfen nur ganz bestimmte USB-Geräte funktionieren. Insbesondere sollen keine beliebigen USB-Geräte verwendet werden können. Auch dürfen keine lokalen Datenspeicher (Weitergabe als "Verzeichnis" oder als "Disk") in der VM verfügbar sein. In einer virtuellen Session aus dem Netzwerk der Stadt Bern (Thin Clients) sollen mehr USB-Geräte zugelassen werden als bei einer Session von ausserhalb (Home Office).

7.3.1.22.1 Durchführung

Der Aufwand für diesen Test war in der verfügbaren Zeit nicht möglich. Recherchen haben das folgende Resultat ergeben.

7.3.1.22.2 Testergebnis

Zunächst müssen die Guest-Tools zwingend im Client installiert sein, dass die USB-Weitergabe überhaupt funktioniert.

USB-Unterstützung (Smartcard, Belegleser, DVD, Smartphones)

- Sobald USB aktiviert ist, können beim Benutzenden eingesteckte USB-Geräte an die Client-VM weitergegeben werden.

Individuelle Rechtevergabe

- Es gibt keine Möglichkeit, für die Weitergabe zu unterscheiden, ob ein Client aus dem internen Netz oder aus dem Internet auf die VM zugreift.

Keine lokalen Laufwerke und USB-Geräte in der Session:

- Es werden keine Laufwerke über SPICE gesendet. USB-Geräte funktionieren nur, wenn der USB-Support aktiviert ist.

7.4 Migrationszenario auf OSS

7.4.1 Erfüllung der Anforderungen

Ein RHV erfüllt die Anforderungen an eine Desktop-Virtualisierung für die Stadt Bern nicht. Mängel sind:

- Kein für Client-Virtualisierung geeigneter Template-Mechanismus
- Kein Support für die Unterscheidung von intern und extern verbundenen Benutzenden
- Kein Support für Feintuning der USB-Weiterleitungen
- Keine Integration von Windows als Gast-Betriebssystem (Profile Manager)
- Kein SSO (wahrscheinlich behebbar)
- Keine Applikationsvirtualisierung.

7.4.2 Auswirkungen auf den IT Betrieb

Aufgrund der Mängel kann RHV nicht anstelle von Citrix eingesetzt werden. Aus den Tests alleine gibt es folgende Punkte, wo mit Mehraufwand oder Mehrverbrauch an Ressourcen zu rechnen ist:

- Upgrades (ein rolling Upgrade ist nicht durchautomatisiert).
- Entwicklung und/oder Instandhaltung von eigenen Lösungen (z.B. mehr VMs, Anpassungen an Client-Applikationen etc)
- Ressourcen Verbrauch: Disk, RAM, CPU

7.4.3 Vendor Lock In

Für Windows-Clients ist die aktuelle Citrix-Virtualisierungslösung ideal und bei der Stadt Bern sehr effektiv umgesetzt. Der Lock In besteht hier schlicht darin, dass keine OSS Lösung notwendigen Funktionsumfang für den Windows-Client- und insbesondere Windows-Applikations-Virtualisierung bietet.

Ein Betrieb von Linux-Clients anstelle von Windows-Clients wäre mit RHV eher möglich. Allerdings kann der Aufwand für eine gleichzeitige Umstellung von Client und Virtualisierungslösung ohne weitergehende Analyse nicht seriös abgeschätzt werden.

7.5 Kostenvergleich

7.5.1 Szenario

Red Hat Virtual Desktop anstatt Citrix Xen Desktop

- Mengengerüst
  - Annahme: ca. 800 FAT Clients
  - Anzahl benötigter CPU's für performanten Betrieb unbekannt, RAM ca. 1.6 - 10 TB, Disk ca. 90 TB
  - Eigentlich 42 Systeme, für concurrent Sessions werden 30 Systeme gerechnet
- Windows Clients
- Aktuell XenPublish, mit RHV VDI volle VM's notwendig, was viel mehr Ressourcen braucht
  - zu beachten insbesondere die Grafik-Power, die unmöglich mehr als 50 gleichzeitige Desktop-Sessions pro Server zulässt.
  - Eventuell mit Hyperconverged Hardware verbesserungsfähig

7.5.2 Investitionen

- **Admin/Support-Schulung:**
  - Annahme: 6 Admins für den Betrieb zu je 6 Tagen Schulung durch einen externen Experten
- **Engineering/Setup:**
  - Einmalige Anschaffung von Hardware (30 Nodes Workernodes, 2 Management Nodes), Storage ähnlich wie mit CitrixXen, deshalb nicht gerechnet
- **Migration / Benutzendenschulung:** Keine Aufwände

Pilot D: Investitionen

		Zusätzliche Investitionen Aufbau OSS Plattform												
		Administratoren / Support Schulung			Engineering / Systemaufbau			Migration (Daten / Schnittstellen)			Benutzer-schulung			Total
Bereich		int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT			0			0			0			0	0
	Basisapplikationen			0			0			0			0	0
	Office Suite (KAT			0			0			0			0	0
	Betriebssystem			0			0			0			0	0
	Hardware			0			0			0			0	0
Netzwerk	WAN			0			0			0			0	0
	LAN			0			0			0			0	0
Data Center	WEB			0			0			0			0	0
	Virtualisierungs-plattform	288	120	65'760	1'200	1'200	414'000			0			0	479'760
	SW Deployment			0			0			0			0	0
	Zentrale Applikationen			0			0			0			0	0
	Datenbank			0			0			0			0	0
	HW / Server / OS			0			0			0			0	0
	RZ Raum/Strom/Klim			0			0			0			0	0
Total				65'760			414'000			0			0	479'760

7.5.3 Betriebskosten

- **Subscriptions**:
  - Externe Betreuung des VDI-Systems durch Schweizer IT-Dienstleister (24/7), stark abhängig von der eigenen Betriebsleistung und dem Grad der Selbständigkeit der Betreuung (Annahme: mittel, eigenständige Betreuung der Hardware)
    - SLA Fixkosten: 15'000 CHF / Jahr
    - Aufwände für Support und Störungsbehebung: 45'000 CHF / Jahr
  - RHV pro Node (>2 Sockets) mit unlimitierter Anzahl Windows Desktops: 1'900 CHF / Jahr
    - Bei 30 Nodes 57'000 / Jahr
- **Betriebsaufwand RZ**: Durch die hohe Anzahl Nodes ebenfalls gerechnet (HE, Strom)
- **Interne Betriebskosten**:
  - Annahme: Die Aufwände für Support und Betrieb bewegen sich in etwa in derselben Grössenordnung wie die Aufwände für den Betrieb von CitrixXen

Pilot D: Betriebskosten

		Reduktion bisheriger Betriebsaufwand / Jahr						Zusätzlicher Betriebsaufwand OSS /				Vergleich
		Lizenzen		Admin / Support			Total	Subscriptions	Admin / Support		Total	
Bereich		Anzahl	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]	ext.	int. [h]	[CHF]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT					0	0			0	0	0
	Basisapplikationen					0	0			0	0	0
	Office Suite (KAT					0	0			0	0	0
	Betriebssystem					0	0			0	0	0
	Hardware					0	0			0	0	0
Netzwerk	WAN					0	0			0	0	0
	LAN					0	0			0	0	0
Data Center	WEB					0	0			0	0	0
	Virtualisierungs-plattform		-140'000			0	-140'000	60'000	200	29'000	89'000	-51'000
	SW Deployment					0	0			0	0	0
	Zentrale Applikationen					0	0			0	0	0
	Datenbank					0	0			0	0	0
	HW / Server / OS					0	0	57'000	1	145	57'145	57'145
	RZ Raum/Strom/Klim					0	0			0	0	0
Total			-140'000			0	-140'000	117'000		29'145	146'145	6'145

7.6 Zusammenfassung

7.6.1 Ergebnisse

Die OSS Variante für eine Client Virtualisierung erfüllt die Anforderungen nicht.

7.6.2 Chancen

- Das grundsätzliche Prinzip der Applikationsvirtualisierung existiert in reinen Unix-Umgebungen (Client und Server) seit etwa 35 Jahren, erfüllt aber weder die heutigen Anforderungen (Ton, USB, …) noch funktioniert es für Windows-Applikationen.

7.6.3 Risiken

- Es gibt zur Zeit kein OSS Produkt, das Windows - Applikationsvirtualisierung unterstützt.

7.6.4 Finanzen

- Durch den Einsatz einer Virtualisierunsplattform, welche die Hardware Resourcen weniger optimal nutzt als Citrix, entstehen zwangsläufig Mehrkosten.

7.6.5 Empfehlung

- Zum heutigen Zeitpunkt kann eine OSS Lösung für die Windows-Applikationsvirtualisierung nicht empfohlen werden
- Die Auswahl von geeigneten Virtualisierungslösungen wird grösser, wenn nicht mehr Windows als Client-Betriebssystem virtualisiert werden muss: Sei es dereinst mit einem OSS-Client oder wenn alle Applikationen in einem Browser laufen.
- Weiteres Beobachtung der Entwicklung

7.6.6 Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Die Funktionalität für eine Client Virtualisierung ist ungenügend.
Sicherstellen des stabilen Informatikbetriebs	Die Stabilität kann mit dem Aufbau von Know How sichergestellt werden. Die Komplexität des Betriebs nimmt zu.
Wirtschaftlichkeit	Die Investitionen in den Plattformaufbau führen zu keinem Return on Investment.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden.

8 Pilotprojekt E: CMI Axioma

8.1 Anforderungsdefinition

CMI Axioma wird von der Stadt Bern für die Verwaltung der politischen Geschäfte benutzt. Allerdings interessiert in diesem Piloten nicht die Sicht der Anwendenden, sondern eine Anpassung der technischen Architektur auf Serverseite.

8.2 Umsetzung

8.2.1 Lösungsansatz

Die Lösung CMI Axioma ist in der aktuellen Version eine klassische "3-Tier" Architektur, bestehend aus den drei Komponenten Client, Applikationsserver und Datenbank. Nach Analyse des Auftrags und Rücksprache mit dem Hersteller (CM Informatik AG[24]) und dem Projekt-Ausschuss wurde folgendes Vorgehen beschlossen:

Das **Client-Programm** wird nicht weiter in die Analyse für das Pilotprojekt einbezogen. CMI ist an der Entwicklung eines HTML-5 basierten Axioma-Clients, welcher mit einem Browser auf einem Linux-Betriebssystem problemlos benutzt werden könnte. Die Zeit arbeitet hier also für OSS.

Es wäre sehr interessant, den **Applikations-Server** auf eine Linux-Plattform zu portieren. Dieser basiert technisch auf Microsoft .net ("dot net“). Leider gibt es für Linux nur die sogenannte ".net core“ Funktionalität. Diese bietet nur einen Teil der Funktionalität von .net – was aber für Axioma nicht reicht.

Bleibt noch die **Datenbank**. Zuerst wurde die Möglichkeit analysiert, auf eine OSS-Datenbank zu wechseln (zB. postgreSQL oder mariaDB). Da sich alle Datenbank-Implementationen jeweils (mehr oder weniger) unterscheiden, wäre dieser Wechsel nicht ohne Anpassungen am Code auf dem Applikations-Server gelungen. Dies hätte also einen substantiellen Beitrag von CMI erfordert. CMI sieht zur Zeit aber keinen Bedarf nach einer Unterstützung von OSS-Datenbanken, eine solche Investition ist also für CMI nicht sinnvoll. Als letzte Möglichkeit, dem Auftrag einigermassen zu entsprechen, wurde immerhin das Betriebssystem des Datenbank-Rechners gewechselt: Es wurde die von Microsoft seit ein paar Jahren angebotene Variante "MSSQL auf Linux“ installiert und mit dem Testsystem verbunden.

8.2.2 Aufbau der Infrastruktur

Die Stadt Bern betreibt für CMI Axioma ein Testsystem, welches für die POTOSS-Tests verwendet werden konnte. Für die Tests wurde ein zusätzlicher virtueller Linux-Server aufgebaut (POT-SQL2026, 2 Cores, 4GB RAM, 50GB Disk) und darauf dann die MSSQL-Datenbank installiert.

8.2.3 Installation der Applikation

Microsoft stellt MSSQL auch als Linux-Paket für RedHat Linux zur Verfügung. Deshalb ist die Installation sehr einfach:

```
# rpm -ivh mssql-server-14.0.3035.2-1.x86_64.rpm
# /opt/mssql/bin/mssql-conf setup
```

Mit dem zweiten Schritt wird das Administratoren-Passwort gesetzt.

8.2.4 Bereitstellen der Testdaten

Die Daten wurden aus der bestehenden Datenbank des Testsystems in die neue Datenbank kopiert. Dies konnte mit der gewohnten Applikation "Microsoft SQL Server Management Studio" durch einen

[24] https://www.cmiag.ch/

Datenbank-Administrator der Stadt Bern durchgeführt werden. Es wurden total vier für die Tests notwendigen Datenbanken kopiert.

8.2.5 Konfigurationen

Auf dem bestehenden Test-Applikations-Server musste lediglich der Datenbankpfad so angepasst werden, dass die Datenbank auf dem Linux-Test-Server benutzt wird.

8.2.6 Funktionstest

Ein rudimentärer Test mit der Axioma Applikation hat vorab bestätigt, dass das Testsystem in der neuen Konfiguration im Wesentlichen funktioniert.

8.3 Testdurchführung

Als vollständiger Test wurde das bereits vorhandene Testszenario "Checkliste Testen Funktionsumfang CMIAXIOMA" durchgespielt. Dieses Szenario wird regelmässig benutzt, z.B. wenn ein neuer Release des CMI Axioma geprüft werden muss.

8.3.1 Testfälle

Sämtliche Testfälle konnten erfolgreich durchgeführt werden. Aus diesem Grund folgen hier nur noch die durchgeführten Tests ohne jeweils einzeln den Erfolg festzuhalten.

8.3.1.1 Geschäftsverwaltung

- Geschäft eröffnen
- Dokument ab Vorlage erstellen, Check-in, Check out
- Verschiedene Dateitypen (Word, Excel, Powerpoint, PDF) importieren. Prüfen, ob Word, Excel und PDF korrekt gerendert werden.
- Dokument elektronisch signieren (z.B. Gemeinderatsantrag).
- Outlook: E-Mails kopieren und in ein AXIOMA-Geschäft ablegen
- Link versenden aus AXIOMA
- E-Mail versenden aus AXIOMA
- Ordner erstellen
- Report testen

8.3.1.2 Aktivitäten

- Aktivität erstellen und innerhalb des eigenen Mandanten versenden. Dokumente sollten an Aktivität gehängt sein.
- Aktivität erstellen mit Dokumenten versehen und an Fremdmandanten senden. Funktioniert das mandantenübergreifende Überweisen? Werden die Aktivitäten synchronisiert?

8.3.1.3 Sitzungsmanagement:

- Sitzung erstellen
- Per Aktivität traktandieren
- Traktanden verschieben
- Traktandenliste erstellen
- Beschlussdokumente generieren
- Beschlussnummern vergeben
- Beschlüsse eröffnen (an Fremdmandanten)

8.3.1.4 Ratssekretariat / Systemadministrator

- Funktioniert Publikation auf RIS und Extranet?
- Geschäft abschliessen
- Sitzung (noch leer) löschen

8.3.1.5 Suche: Eigener Mandant / Mandant GR

- Eigener Mandant: Nach Geschäft, Dokument und Aktivität suchen
- Mandant GR: Sitzung anschauen (sofern berechtigt), GRB und GRA suchen, Suche nach geheimen Dokumenten ohne Treffer (ausser Berechtigung vorhanden).

8.4 Migrationszenario auf OSS

CMI Axioma kann technisch nur dann auf OSS-Plattformen laufen, wenn das der Hersteller CMI unterstützt. Dazu müsste CMI den Quellcode von Axioma selbst nicht unbedingt offenlegen, aber doch umfangreiche Anpassungen an der Applikation vornehmen. Dazu kommt zusätzliche Testinfrastruktur, erhöhter Supportaufwand, etc.

8.4.1 Erfüllung der Anforderungen

Die notwendigen Anpassungen an Axioma wären rein technischer Natur. Es ist davon auszugehen, dass der volle Funktionsumfang auch in einer Version, die auf OSS Plattformen läuft, zur Verfügung gestellt werden kann.

8.4.2 Auswirkungen auf den IT Betrieb

Die Stadt Bern setzt bereits heute Linux ein, es gibt einen Prozess zur Bereitstellung von CentoOS Servern. Eine Migration von CMI Axioma auf OSS hätte kaum Auswirkungen auf den Betrieb.

8.4.3 Benutzendenschulungen

Für die Benutzenden würde sich nichts ändern, es wären keine zusätzlichen Schulungen notwendig.

8.4.4 Vendor Lock In

CMI Axioma ist auf Windows als Server-Plattform beschränkt. Eine Portierung auf eine OSS-Plattform ist für den Hersteller wegen mangelnder Nachfrage nicht interessant. Solange CMI Axioma das einzige Tool ist, welches die Anforderungen erfüllt, ist die Stadt Bern punkto Plattform von den Entscheidungen des Herstellers abhängig.

8.5 Kostenvergleich

8.5.1 Szenario

MSSQL-Datenbanken auf Linux- anstatt Windows-Servern

- Mengengerüst:
  - Ein Datenbankserver mit 9 Datenbanken für die Applikation Axioma

8.5.2 Investitionen

- **Setup**: Hängt ab vom Automatisierungsgrad der Verwaltung.
  - Annahme für Installation und Integration (OS und DB): 2 Tage
  - Es wird davon ausgegangen, dass die Stadt Bern selber ein Linux ausrollen kann

- **Migration Applikation**: Wiederum abhängig vom Komplexitätsgrad. Organisation von Downtimes etc. mit einbezogen wird das zwischen 4 und 8 Stunden Aufwand machen.
- **Betreiber-Schulung**: Kein Schulungsaufwand für MSSQL und Linux Basis-OS.
- **Benutzendenschulung**: Für den Benutzenden ändert sich nichts. Keine Mehrkosten erkennbar

Pilot E: Investitionen

		Zusätzliche Investitionen Aufbau OSS Plattform												
		Administratoren / Support Schulung			Engineering / Systemaufbau			Migration (Daten / Schnittstellen)			Benutzer-schulung			Total
Bereich		int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT			0			0			0			0	0
	Basisapplikationen			0			0			0			0	0
	Office Suite (KAT			0			0			0			0	0
	Betriebssystem			0			0			0			0	0
	Hardware			0			0			0			0	0
Netzwerk	WAN			0			0			0			0	0
	LAN			0			0			0			0	0
Data Center	WEB			0			0			0			0	0
	Virtualisierungs-plattform			0			0			0			0	0
	SW Deployment			0			0			0			0	0
	Zentrale Applikationen			0			0			0			0	0
	Datenbank			0	4		580	6		870			0	1'450
	HW / Server / OS			0	12		1'740	0		0			0	1'740
	RZ Raum/Strom/Klim			0			0			0			0	0
Total				0			2'320			870			0	3'190

8.5.3 Betriebskosten

- **Wiederkehrende Lizenzkosten**: Applikationskosten bleiben unverändert.
  - RHEL Standard Subscription 2-sockets 763 CHF (1 Jahr)
- **Interner Betrieb**: Fallen in der gleichen Höhe an, wie für den Betrieb auf Windows.

Pilot E: Betriebskosten

		Reduktion bisheriger Betriebsaufwand / Jahr						Zusätzlicher Betriebsaufwand OSS /				Vergleic
		Lizenzen		Admin / Support			Total	Subscriptions	Admin / Support		Total	
Bereich		Anzahl	[CHF]	int. [h]	ext. [h]	[CHF]	[CHF]	ext.	int. [h]	[CHF]	[CHF]	[CHF]
Clients	Fachapplikationen (KAT 3 und KAT					0	0			0	0	0
	Basisapplikationen					0	0			0	0	0
	Office Suite (KAT					0	0			0	0	0
	Betriebssystem					0	0			0	0	0
	Hardware					0	0			0	0	0
Netzwerk	WAN					0	0			0	0	0
	LAN					0	0			0	0	0
Data Center	WEB					0	0			0	0	0
	Virtualisierungs-plattform					0	0			0	0	0
	SW Deployment					0	0			0	0	0
	Zentrale Applikationen					0	0			0	0	0
	Datenbank					0	0	0		0	0	0
	HW / Server / OS					0	0	760		0	760	760
	RZ Raum/Strom/Klim					0	0			0	0	0
Total			0			0	0	760		0	760	760

8.6 Zusammenfassung

8.6.1 Ergebnisse

Der Hersteller von CMI Axioma bietet keine Variante, welche unter einem OSS Betriebssystem lauffähig ist. Die einzige Möglichkeit besteht darin, die Datenbank auf Linux zu portieren.

8.6.2 Chancen

Der Einsatz von OSS anstelle von proprietärer Software bietet im Pilotprojekt E folgende Chancen:

- Portieren der Datenbank auf ein Linux System
- Lösen der Abhängigkeit von marktdominanten Herstellern
- Kleiner Schritt Richtung OSS

8.6.3 Risiken

Der Einsatz eines OSS Betriebssystem birgt im Pilotprojekt E keine erkennbaren Risiken.

8.6.4 Finanzen

- Keine Einsparung von Microsoft Windows Lizenzen
- Investitionen in die Datenbank Migration

8.6.5 Empfehlung

- Keine Migration der Datenbank auf Linux, kein Gewinn.

8.6.6 Übersicht

Kriterium	Begründung
Funktionalität für die Geschäftsabwicklung	Die Funktionalität ist durch die Portierung auf ein OSS Betriebssystem nicht tangiert
Sicherstellen des stabilen Informatikbetriebs	MS SQL wird für Linux angeboten. Der Support durch CMI AXIOMA ist nicht gewährleistet.
Wirtschaftlichkeit	Investition in die Datenbank-Migration. Keine Einsparung von Lizenzkosten.
Abhängigkeit von dominanten Marktteilnehmenden	Die Abhängigkeit von den grossen Marktteilnehmenden kann nicht gelöst werden. Ein erster Schritt wäre möglich.

9 Strategische Aspekte

9.1 Ursachenanalyse

Die Analyse hat gezeigt, dass bei den konkret untersuchten Pilotprojekten ein günstigerer Betrieb durch einen Umstieg auf Open Source Software nicht möglich ist. Es gibt zwei tiefere Gründe für dieses ernüchternde Fazit.

9.1.1 Fehlende Eigenschaften der Alternativen

Im Pilot C und vor allem D wurde festgestellt, dass den OSS-Alternativen wichtige technische Funktionen fehlen.

In allen Pilotprojekten stellte sich früher oder später die Frage, ob der Support für gewisse Umsysteme noch gewährleistet sei, wenn man Teile des Gesamtsystems einfach ersetzt.

9.1.2 Enge Kopplung

Eine ICT-Infrastruktur wie die der Stadt Bern besteht aus Tausenden von Komponenten, die alle bis zu einem gewissen Grad zusammenarbeiten müssen.

In allen untersuchten Bereichen konnte eine enge Koppelung zwischen Applikation, Datenformat, Betriebssystem und Client-Virtualisierung festgestellt werden. Jede Änderung an einer Komponente beeinflusst auch die anderen (Pilot A/B/D).

Oft ist eine Applikation nur für eine bestimmte Plattform verfügbar (Pilot B/E), dies kann als Extremfall dieser Koppelung betrachtet werden.

9.2 Strategien

9.2.1 Fehlende Eigenschaften

Beim Piloten D (Virtualisierung) waren die zu Beginn des Projekts verfügbaren OSS-Virtualisierungs-lösungen nicht für Client-Virtualisierung geeignet – die Tests haben das mehr als bestätigt. Es sieht zwar so aus, als ob sich die Situation in den letzten zwei Jahren verbessert hat und entsprechende OSS Produkte entwickelt wurden. Trotzdem ist zu erwarten, dass Citrix noch eine Weile die Messlatte für Windows-Clientvirtualisierung bleibt.

Beim Piloten C (Email) haben wir die Empfehlung „der Browser ist das Betriebssystem“ praktisch getestet, indem wir ausschliesslich den Web-Client von OX geprüft haben. Die Ergebnisse waren soweit gut, aber das fehlende „send on behalf of“ Feature macht OX ungeeignet für den Einsatz in einer Verwaltung. Dazu kommen die Supportprobleme mit Umsystemen.

Folgende Massnahmen könnten helfen, mehr OSS Software in der Stadt Bern einsetzen zu können:

- Vorantreiben eines Entscheids: kann eine IT-Landschaft nur mit Web-Applikationen den Anforderungen genügen? Die Freiheit vom Betriebssystem wird abgelöst durch die Abhängigkeit vom Netzwerk. Offline Arbeiten wäre dann nicht mehr möglich. Oder welche Ausnahmen müssten gewährt werden, um das Ziel wenigstens für «fast alle» zu erreichen?
- Software-Beschaffung/Erneuerung:
    - Vor jedem grösseren Lifecycle (z.B. Ersatz der Desktops) werden aktuelle Informationen über den Stand der Entwicklung bei OSS eingeholt und – bei «guten» Chancen – ein Wechsel genauer analysiert.
    - Bei Eigenentwicklungen: Als OSS entwickeln lassen. Gemeinsamen Nutzen mit anderen Behörden suchen.
    - Zusammenarbeit mit einem OSS Hersteller: Features wie «send on behalf of» können zu Programmierung in Auftrag gegeben werden. Dabei muss sichergestellt werden, dass die

Anpassung permanent ins Produkt einfliesst und langfristig gepflegt wird. Solche Fragen sollten bereits bei der Voranalyse geklärt werden.

9.2.2 Enge Kopplung

Die Kopplung zwischen Komponenten (Hardware, Betriebssystem, Applikationen) kann auf grundsätzlich zwei verschiedene Arten erfolgen. Diese werden im Folgenden „Schnittstellen“ bzw. „Dateiformate“ genannt.

Bei Schnittstellen geht es um **übertragene** Daten, bei Dateiformaten um **gespeicherte** Daten.

Bei einer Schnittstelle kommunizieren zwei Komponenten direkt miteinander, Beispiele dafür sind:

- Word ruft Outlook auf um ein bearbeitetes Dokument zu verschicken
- Ein Browser ruft eine Webseite auf und stellt sie dar

Dateiformate bestimmen, wie Informationen «eingefroren» werden, damit sie später wieder benutzt werden können. Beispiele dafür sind:

- Format einer Word-Datei (.docx)
- Format einer PDF-Datei (.pdf)

Ob Daten übertragen oder gespeichert werden, hat verschiedene Implikationen, die Wichtigsten sind:

Übertragene Daten sind per Definition flüchtig, das heisst bei einem Wechsel der Schnittstelle gibt es keine Daten, die zu migrieren wären. Dafür sind bei Schnittstellen immer (mindestens) zwei aktive Komponenten beteiligt, das heisst bei einem Wechsel müssen alle beteiligten Komponenten gleichzeitig angepasst werden.

Bei gespeicherten Daten ist es «umgekehrt»: Bei einem Wechsel des Datenformats muss der gesamte Datenbestand migriert werden, dafür muss der Wechsel nicht auf einen Schlag passieren (alte Daten werden mit dem alten, neue Daten mit dem neuen Programm bearbeitet).

9.2.2.1 Schnittstellen

Auf dem Windows-Desktop gibt es (historisch bedingt) eine Unmenge an Schnittstellen, die zwischen den Applikationen genutzt werden können. Solange wesentliche Geschäftsprozesse an diese Schnittstellen gebunden sind, wird eine Abkehr von Windows auf dem Desktop nicht möglich sein.

Mittelfristig könnte daran gearbeitet werden, einem Teil der Mitarbeitenden einen Linux-Desktop zur Verfügung zu stellen. Crossover als Hilfstechnologie scheidet aber aus Support-Gründen aus, das Darstellungsproblem von Citrix-Applikationen muss noch gelöst werden. Ein Parallelbetrieb ist zwar interessant um Erfahrungen zu sammeln, aber nicht kostenneutral.

Langfristig kann diese Abhängigkeit nur dadurch gelöst werden, dass konsequent auf Web-Applikationen gesetzt wird. Wichtig dabei ist:

- Nur echte Web-Applikationen sind gute Web-Applikationen. Sie müssen also eine breite Palette von Client-Betriebssystemen und Browsern unterstützen. Dazu können bei der Beschaffung geeignete Architektur-Vorgaben gemacht werden.
- Die Web-Applikationen müssen ein dokumentiertes und stabiles (bzw. versioniertes) API anbieten, welches die Kommunikation zwischen Web-Applikationen ermöglicht (und damit die Betriebssystem-Schnittstellen ablösen kann).

Der OX-WebClient (Pilot C) erfüllt zum Beispiel beide Anforderungen.

Langfristig führt diese Strategie zu einer Infrastruktur, wo die Benutzenden völlig unabhängig vom Betriebssystem Ihre Aufgaben erledigen können. Anders ausgedrückt: Neu ist der Browser das Betriebssystem.

9.2.2.2 Dateiformate

Die digitalen Resultate der täglichen Arbeit bei der Stadt Bern werden in verschiedensten Datei-Formaten gespeichert. Als Gedankenexperiment bemessen wir den Wert einer gespeicherten Datei an der Zeit, die gespart wird, wenn sie ein zweites Mal verwendet wird. Hat zum Beispiel das Verfassen eines Briefs zwei Stunden gedauert und der nächste ähnliche Brief konnte dank dieser Vorlage in nur einer Stunde verfasst werden, dann hatte die gespeicherte Datei einen Wert von einer Stunde. Der Wert einer Datei hängt also davon ab, wie viel Zeit investiert wurde und ob sie ein weiteres Mal verwendet wird. Je länger die letzte Verwendung einer Datei her ist, desto weniger wahrscheinlich ist es, dass sie nochmal benutzt wird. Es gibt also auch in diesem Modell so etwas wie „Abschreibung“.

9.2.2.2.1 Monokultur

Im praktischen Alltag hat die Stadt Bern durch die flächendeckende Verwendung von .docx zwei Vorteile:

- Der intensive interne und externe (z.B. Bund, Kanton) Austausch von Dokumenten funktioniert praktisch reibungslos – der Wert der Dateien bleibt erhalten. Dieser Vorteil liegt vor allem an der grossen Verbreitung von Microsoft Office und nicht etwa an der mangelnden Qualität von LibreOffice.
- Eine uniforme IT-Infrastruktur ist einfacher und damit günstiger.

Die Microsoft Monokultur hat aber auch eine Reihe von Nachteilen:

- Malware kann sich einfach und über Systemgrenzen ausbreiten. Es ist wesentlich einfacher, einen Virus für eine bestimmte Version MS-Word zu schreiben als einen Virus, der sowohl unter MS-Word als auch LibreOffice funktioniert. Das ist der Nachteil einer uniformen Infrastruktur.
- Wie kann sichergestellt werden, dass die Resultate unserer Arbeit in 10 oder 20 Jahren noch lesbar sind?
- Die Lizenzgebühren für proprietäre Software fliessen zum grössten Teil an Firmen, die in der Schweiz keine oder kaum Steuern zahlen.
- Auch Know-how wird tendenziell ausserhalb der Schweiz gefördert.

Während die Vorteile betriebswirtschaftlich direkt einsichtig sind, sind die Nachteile eher langfristiger und volkswirtschaftlicher Natur.

9.2.2.2.2 Vendor Lock In

Das Hauptproblem von Dateien in einem proprietären Format liegt darin, dass sie nur von (closed source) Programmen eines Herstellers interpretierbar sind. Die Microsoft-Office-Formate sind zwar de jure „offene Standards“, d.h. das Dateiformat „.docx“ ist (in einer 6000 Seiten umfassenden Spezifikation) offengelegt. De facto gibt es aber bis jetzt keine OSS-Software, die absolut problemlos .docx Dateien liest und schreibt. Es ist sogar so, dass Microsoft Word auf macOS und Microsoft Word auf Windows unterschiedliche Resultate liefern können. Deshalb werden die Microsoft-Office-Format hier wie proprietäre Formate behandelt.

Die Stadt Bern ist von Microsoft in dem Sinne abhängig, dass ein Wechsel zu einem anderen Produkt immer mindestens den Wert aller gespeicherten Dateien kostet.

Es ist davon auszugehen, dass Firmen, die "Massensoftware" (Betriebssysteme, Office-Programme) verkaufen, sich dieser Problematik durchaus bewusst sind und ihre Preisgestaltung auch an den Migrationskosten der Kunden orientieren: Der Preis ist so hoch wie möglich, aber doch deutlich unter potentiellen Migrationskosten.

9.2.3 Massnahmen

9.2.3.1 Elektronischer «Aktenplan»

Eine Migration zu OpenSource Formaten wird sich kurzfristig nicht auszahlen. Trotzdem kann es sinnvoll sein, die Formatproblematik ganzheitlich anzuschauen. Dazu gehört mindestens

- Ein Inventar der benutzten Formate und der zugehörigen Geschäftsprozesse.
- Eine Bewertung der Formate nach verschiedenen Kriterien wie zum Beispiel „nicht geeignet für Langzeit-Archivierung“ oder „nicht im Austausch mit Bürgern verwenden“.
- Abstimmung mit anderen Verwaltungen (Kanton, Bund).

Daraus können interne Richtlinien abgeleitet werden. Es wäre zum Beispiel möglich, alle Word-Dateien nur noch in .ODT (statt .DOCX) zu speichern. Oder bei neuen Vorlagen zu fordern, dass sie auch in LibreOffice funktionieren. Dies macht aber nur Sinn, wenn diese Richtlinien auf eine langfristige Strategie abgestimmt sind.

9.2.3.2 Anpassung Auftrag

Der Betreiber einer IT Infrastruktur hat grundsätzlich drei übergeordnete Ziele:

1. Bereitstellen aller Funktionalität, welche für die Geschäftsabwicklung durch die Benutzenden erforderlich ist
2. Sicherstellen eines stabilen und reibungslosen IT Betriebs
3. Anbieten dieser IT Infrastruktur und Dienstleistungen zu minimalen Kosten

Diese Ziele müssen im Alltag immer wieder gegeneinander abgewogen und optimiert werden. Bei einer Einführung von OSS im Sinne der Pilotprojekte müssten in allen Bereichen Einschränkungen in Kauf genommen werden.

Es ist letztlich ein politischer Entscheid, ob der (nicht unmittelbar in Geld messbare) Gewinn an Sicherheit, Langzeitverfügbareit, Know-how, Unabhängigkeit etc. durch eine Abkehr von proprietären Datenformaten den Mehraufwand wert ist. Es geht um die «Digitale Souveränität» der öffentlichen Verwaltungen.

Ist dies gewünscht, müsste die Politik den Leistungsauftrag der Betreiber um einen Punkt ergänzen:

> *Weitgehende Kontrolle über die von der Verwaltung erzeugten Daten (z.B. Speichern von kritischen Daten nur in offengelegten Formaten)*

Der vorliegende Bericht zeigt auf, wo die Möglichkeiten und Grenzen einer Weiterentwicklung in diesem Bereich für die Stadt Bern bestehen.