

Beschlussvorlage für Ausschüsse



Landeshauptstadt
Mainz

öffentlich		Drucksache Nr. 1090/2025
Amt/Aktenzeichen 16/16/Dezernat I/16-KDZ/16 01 01	Datum 31.07.2025	TOP 3

Beratungsfolge Gremium	Zuständigkeit	Datum	Status
Werkausschuss der Kommunalen Datenzentrale Mainz	Entscheidung	20.08.2025	Ö

Betreff:

Vergabeangelegenheit
hier: Beschaffung von IT-Arbeitsplatzsoftware (Microsoft 365, Teams und Supportverlängerung Windows 10)

Mainz, 13. August 2025

gez.
Nino Haase
Oberbürgermeister

Beschlussvorschlag:

Der Werkausschuss der Kommunalen Datenzentrale Mainz stimmt der Beschaffung der notwendigen IT-Arbeitsplatzsoftware „Microsoft 365“ zu.

Anwendung findet grundsätzlich die Version E3 mit EMS E5 (571 €/User), ausnahmsweise die Version E5 (644 €/User). Gleichzeitig ist während der Einführung eine Supportverlängerung für Windows 10 (43,00 €/User) erforderlich.

Beabsichtigt ist die spätere Erweiterung um „Teams“ (ca. 65,00 €/User).

Alle Preisangaben verstehen sich pro Jahr, inklusive Umsatzsteuer.

Bei weiterer Nutzung dieser Software werden diese „Lizenznutzungskosten“ mit den dann geltenden Gebühren fortgesetzt.

Problembeschreibung/ Begründung:

1. Sachverhalt

Als IT-Dienstleister der Stadtverwaltung Mainz und stadtnaher Gesellschaften ist die KDZ Mainz verpflichtet, auf eine ordnungsgemäße Lizenzierung der IT-Standard-Arbeitsplätze zu achten. Die eingesetzten Softwareprodukte müssen, z. B. aus Gründen der IT-Sicherheit, stets aktuell gehalten werden.

Hierzu stellt die KDZ Mainz den Betrieb für zurzeit ca. 3.300 Endgeräte (mit zunehmender Tendenz durch Schaffung neuer Arbeitsplätze/Stellen) mit der entsprechenden Standardarbeitsplatzsoftware, wie z. B. MS Office, Windows-Betriebssystem, sicher.

Bisher wurden die Endgeräte regelmäßig zusammen mit den vergünstigten Windows-Professional-Lizenzen erworben, die den gestiegenen Sicherheits- und Administrationsanforderungen nicht mehr entsprechen. Darüber hinaus wurden für MS-Office (teilweise gebrauchte) Lizenzen erworben.

Da die bisher eingesetzten Windows- und Office-Versionen ab dem 14. Oktober 2025 keine Updates mehr durch Microsoft erhalten, ist die Umstellung auf aktuelle Versionen notwendig. Aufgrund dessen hat die Stadtverwaltung entschieden, auf Microsoft 365 umzustellen, was automatisch fortwährend die jeweils aktuellen Versionen von Windows und Office beinhaltet.

Dadurch ändert sich die Art der Lizenzbeschaffung. Während die Lizenzen bisher einmalig beschafft und bezahlt wurden (Kaufmodell), beinhaltet Microsoft 365 ein Abo-Modell, dass wahlweise monatlich oder jährlich zu bezahlen ist. Es besteht die Option, das Abonnement jederzeit zum Ende der jeweiligen Laufzeit zu kündigen.

Aufgrund der Empfehlung der bridgingIT sollen die Versionen „E3“ mit EMS E5 und bei besonderen Anforderungen „E5“ zum Einsatz kommen.

Beabsichtigt ist die spätere Erweiterung um „Teams“ als Kollaborationssoftware.

Wie zuvor bereits erwähnt, endet der Updatezyklus für die aktuell eingesetzten Windows- und Office-Versionen im Oktober 2025. Da eine Umstellung auf eine aktuellere Windows-Version bis zu diesem Zeitpunkt nicht abgeschlossen sein wird, sollen Lizenzen für eine Verlängerung des Updatezyklus erworben werden. Die Kosten für diese Verlängerungslizenzen belaufen sich auf ca. 43,00 € brutto pro Arbeitsplatz, und betragen somit 141.900,00 € brutto für ein Jahr.

Für Office besteht keine Möglichkeit einer Supportverlängerung.

In der KDZ-Werkausschusssitzung am 20.03.2025 wurde die Entwicklung einer IT-Strategie zur DSGVO-konformen Einführung von Microsoft 365 mit einem externen Dienstleister mit Ergänzungen beschlossen (BV 0027/2025). Die Stellungnahme zu diesen Ergänzungen können der Anlage entnommen werden.

2. Lösung

Der Werkausschuss der Kommunalen Datenzentrale Mainz stimmt der Beschaffung der notwendigen IT-Arbeitsplatzsoftware „Microsoft 365“ zu.

Anwendung findet grundsätzlich die Version E3 mit EMS E5 (571€/User), ausnahmsweise die Version E5 (644€/User). Gleichzeitig ist während der Einführung eine Supportverlängerung für Windows 10 (43,00 €/User) erforderlich.

Beabsichtigt ist die spätere Erweiterung um „Teams“ (ca. 65,00 €/User).

Alle Preisangaben verstehen sich pro Jahr, inklusive Umsatzsteuer.

Bei weiterer Nutzung dieser Softwares werden diese „Lizenznutzungskosten“ mit den dann geltenden Gebühren fortgesetzt.

3. Alternativen

Ein Weiterbetrieb der derzeit verwendeten Produkte (MS Windows 10 und MS Office 2016) würde ohne Updates erfolgen und ein erhebliches Risiko für die Datensicherheit der Stadtverwaltung Mainz darstellen. Zudem wären die neuen Anforderungen an kollaboratives Arbeiten und zukunftsfähige Arbeitsplätze nicht erfüllbar, was absehbar die Leistungsfähigkeit der Verwaltung einschränken würde.

4. Ausgaben/Finanzierung

Diese Lizenznutzungskosten sind im Wirtschaftsplan der KDZ Mainz berücksichtigt. Die Refinanzierung erfolgt über entsprechende Kontrakte mit der Stadtverwaltung Mainz und Verträgen/ Vereinbarungen mit stadtnahen Gesellschaften.

Anlage

Stellungnahme zum Beschluss (BV 0027/2025):

1. *Die von dem beauftragten Unternehmen zu erarbeitende Strategie soll Maßnahmen zur Gewährleistung eines dem Schutzbedarf der verarbeiteten Daten angemessenen Sicherheitsniveaus umfassen. Dies beinhaltet insbesondere:*
 - a) *Die Speicherung und Verarbeitung der Daten unter Berücksichtigung geltender Datenschutz- und Sicherheitsanforderungen, insbesondere hinsichtlich des Zugriffs durch unbefugte Dritte.*

Aktueller Sachstand hierzu:

- Die Speicherung und Verarbeitung von Daten in Microsoft 365 erfolgt unter strenger Berücksichtigung geltender Datenschutz- und Sicherheitsanforderungen. Microsoft betreibt seine Cloud-Dienste nach dem Prinzip der geteilten Verantwortung, wobei der Schutz der Infrastruktur, der Plattform und der Dienste durch Microsoft gewährleistet wird, während die KDZ für die Konfiguration und Verwaltung der Datenzugriffe verantwortlich ist. In der bestehenden Microsoft 365 Umgebung wurde bereits eine Basis-Härtung des Tenants vorgenommen, um unbefugten Zugriff konsequent zu unterbinden.
- Ein zentrales Element dieser Absicherung ist die Customer Lockbox, die sicherstellt, dass Microsoft-Mitarbeitende nur dann auf Kundendaten zugreifen können, wenn dies durch die KDZ explizit genehmigt wird. Selbst im Rahmen von Supportfällen oder Wartungsarbeiten ist ein Zugriff ohne vorherige Freigabe durch autorisierte Personen der KDZ nicht möglich. Sämtliche Zugriffe seitens Microsoft auf den Microsoft 365 Tenant der KDZ werden im sog. Auditlog protokolliert. Die Logs stehen den Globalen Administratoren zur Verfügung und können von diesen jederzeit ausgewertet werden.
- Darüber hinaus wurde eine Zugriffsstruktur mittels Conditional Access implementiert, die den Zugriff auf die Microsoft 365-Dienste streng reglementiert. Dabei werden verschiedene Bedingungen wie Benutzeridentität, Gerätestatus, Standort und Risikobewertung berücksichtigt. Diese Richtlinien ermöglichen es, Bedrohungen wie Identitätsdiebstahl oder den Zugriff über kompromittierte Geräte effektiv zu unterbinden.
- Ebenso wurden die Funktionen zum anonymen Teilen von Inhalten deaktiviert und sind streng reglementiert. Dadurch wird sichergestellt, dass Daten nur gezielt und nachvollziehbar mit bestimmten Personen oder Gruppen geteilt werden können.
- Ergänzend dazu können ggf. im Rahmen eines Enterprise Agreements (EA) mit Microsoft weitere vertragliche Regelungen getroffen werden, die zusätzliche Sicherheits- und Datenschutzanforderungen abdecken.

- b) *Die regelmäßige Bereitstellung geprüfter Updates, um die Integrität und Sicherheit der Anwendung sicherzustellen.*

Aktueller Sachstand hierzu:

- Bei der Nutzung der Microsoft 365-Dienste sowie den Microsoft 365 Apps for Enterprise stellt Microsoft sicher, dass sowohl die Integrität als auch die Sicherheit der Dienste und Anwendungen kontinuierlich gewährleistet sind.
- Die cloudbasierten Dienste von Microsoft 365 – darunter Exchange Online, SharePoint Online, Microsoft Teams und weitere – werden vollständig von Microsoft betrieben und regelmäßig aktualisiert. Diese Updates erfolgen automatisch im Hintergrund, ohne dass ein manuelles Eingreifen durch die KDZ erforderlich ist. Über das Microsoft 365 Message Center sowie die Microsoft 365 Roadmap wird frühzeitig über geplante Änderungen informiert. Weiteres hierzu wird im Konzept zur Einführung von Microsoft 365 unter „M365 Evergreen Management“ beschrieben werden. Im Microsoft 365 Message Center werden hierzu tenantspezifische Informationen zu den ausstehenden bzw. geplanten Änderungen in Microsoft 365 mit entsprechendem zeitlichem Vorlauf kommuniziert und evtl. Änderungen für die Benutzer beschrieben. Die Microsoft Roadmap hingegen gibt einen längerfristigen Überblick über die kommenden Änderungen, enthält geschätzte Veröffentlichungstermine und Beschreibungen und wie bei jeder Roadmap können sich alle Informationen ändern. Die Informationen in der Microsoft Roadmap sind nicht tenantspezifisch und betreffen immer den kompletten Microsoft 365 Service.
- Die Microsoft 365 Apps for Enterprise –die lokal installierten Office-Anwendungen wie Word, Excel oder PowerPoint – erhalten regelmäßig Updates, die sowohl neue Funktionen als auch sicherheitsrelevante Korrekturen enthalten. Über die sogenannten Update-Kanäle kann zwischen verschiedenen Update-Zyklen gewählt werden, je nachdem, wie häufig neue Funktionen bereitgestellt werden sollen: Vom Current Channel mit monatlichen Updates bis hin zum Semi-Annual Enterprise Channel mit halbjährlichen Aktualisierungen. Diese Aktualisierung findet in der KDZ über die bestehende Infrastruktur mittels Matrix42 Empirum statt.

- c) *Die Verschlüsselung gespeicherter Daten (Dateien, E-Mails etc.), angepasst an den jeweiligen Schutzbedarf.*

Aktueller Sachstand hierzu:

- In einer Microsoft 365 Umgebung werden gespeicherte Daten wie Dateien, E-Mails und andere Inhalte standardmäßig verschlüsselt – sowohl im Ruhezustand („at rest“) als auch während der Übertragung („in transit“). Microsoft verwendet dabei eine Kombination aus serviceeigener Verschlüsselung auf Dateiebene und Transport Layer Security (TLS), um die Daten umfassend zu schützen.
- Für Daten im Ruhezustand bedeutet das, dass Inhalte, die in Diensten wie SharePoint Online, OneDrive for Business oder Exchange Online gespeichert sind, automatisch mit starken Verschlüsselungsalgorithmen wie AES-256 gesichert werden.
- Für in Exchange Online gespeicherte Daten steht zusätzlich das Microsoft Verfahren OME (Office Message Encryption) zur Verfügung. Mit diesem können Emails für Empfänger ähnlich wie mit S/MIME verschlüsselt werden. Somit kann sichergestellt werden, dass nur berechtigte Empfänger die Emails incl. der enthaltenen Dateianhänge öffnen. Die Verschlüsselung ist unabhängig vom Speicherort und unveränderlich mit den geschützten Dokumenten verbunden.

- Bei der Übertragung von Daten – etwa beim Zugriff auf E-Mails über Outlook oder beim Hochladen von Dateien in Teams – sorgt TLS dafür, dass die Kommunikation zwischen dem Endgerät und den Microsoft-Servern geschützt ist.
- Standardmäßig werden in einem Microsoft 365 Tenant die Root-Schlüssel von Microsoft bereitgestellt und verwaltet. Bei erhöhtem Schutzbedarf können zusätzliche Verschlüsselungsmechanismen (teilweise verbunden mit Zusatzkosten) für den Microsoft 365 Tenant der KDZ eingerichtet und genutzt werden. Folgende zusätzliche Verschlüsselungsverfahren stehen zur Verfügung:
 - Customer Key ist eine kundenseitig verwaltete Schlüssellösung, bei dieser werden die Root-Schlüssel, die zur Verschlüsselung der Dienste verwendet werden, vom Kunden zur Verfügung gestellt und in Azure Key Vault verwaltet. Microsoft verwaltet alle anderen Schlüssel.
 - Double Key Encryption (DKE) ist eine Lösung zum Schutz hochsensibler Daten. Mit dieser Lösung mit DKE behält der Kunde die Kontrolle über die eingesetzten Verschlüsselungsschlüssel. Es werden zwei Schlüssel zum Schutz der Daten verwendet: ein Schlüssel unter Kontrolle des Kunden und ein zweiter Schlüssel, der sicher in Microsoft Azure gespeichert wird. Für die Anzeige von Daten, die mit Double Key Encryption geschützt sind, ist der Zugriff auf beide Schlüssel erforderlich.
 - Der Double-Key-Verschlüsselungsdienst, mit dem die Kundenschlüssel angefordert werden, kann entweder in entsprechenden Schlüsselverwaltungsservern (HSM-Modul) vor Ort oder in entsprechenden Schlüsselverwaltungsservern in der Cloud verwaltet werden.
 - Entsprechende HSM-Module werden beispielsweise von Thales und anderen Anbietern wie Entrust bereitgestellt.
 - Die Thales Dokumentation ist erreichbar unter <https://cpl.thalesgroup.com/de/cloud-security/encryption/double-key-encryption>.
 - Die Entrust Dokumentation ist erreichbar unter <https://www.entrust.com/sites/default/files/documentation/datasheets/hsm-double-key-encryption-azure-information-protection-ds.pdf>.
- Die HSM-Module unterstützen bei der Einhaltung interner Richtlinien und gesetzlicher Vorschriften wie der DSGVO, HIPAA und Schrems II, indem die kryptographischen Masterschlüssel separat von den sensiblen Daten in einem HSM gespeichert werden.

d) Die Strategie ist unter Berücksichtigung der C5-Testierung (Typ 2) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu erstellen, um den Schutzbedarf der verarbeiteten Daten angemessen zu berücksichtigen.

Aktueller Sachstand hierzu:

- Die bereits umgesetzten Basis-Härtungsmaßnahmen wurden anhand des BSI IT-Grundschutz, ISO / IEC 27001 sowie der CIS M365 Benchmark V4.0 umgesetzt. Weitere Diensthärtungsmaßnahmen werden im Konzept zur Einführung von Microsoft 365 beschrieben werden.
- Zur regelmäßigen Bewertung der Umgebungsabsicherung bietet Microsoft sog. Initiativen, in welchen der aktuelle Sicherheitsstatus sowie die Veränderung (Trend) geprüft werden können. Zu den Initiativen gehören Prüfungen der gesamten Umgebung sowie spezielle Prüfungen, zugeschnitten auf aktuelle Angriffsvektoren.
- Das aktuelle C5 Testat für Microsoft 365 und Azure ist hier zum Download verfügbar: <https://servicetrust.microsoft.com/DocumentPage/0e782c1d-9ca9-4d28-ba9f-263f3c359f28>
- Die entsprechenden Dokumente für die Einhaltung der DSGVO, insbesondere im Bereich der öffentlichen Auftraggeber, sind hier zu finden: <https://servicetrust.microsoft.com/viewpage/GDPR>

- Weitere Dokumente mit Bedeutung für Unternehmen und öffentliche Auftraggeber in Deutschland sind im Microsoft Trust Center hier zu finden:
<https://servicetrust.microsoft.com/ViewPage/RegionalGermany>

e) *Eine Kostenkalkulation für Migration und Betrieb, unter Berücksichtigung langfristiger wirtschaftlicher Planbarkeit.*

Aktueller Sachstand hierzu:

- Die Migrationskosten selbst sind schwer pauschal zu beziffern. Sie hängen maßgeblich von der Anzahl und Komplexität der zu migrierenden Anwendungen, der Datenvolumina, der Integrationsanforderungen sowie dem Schulungsbedarf der Mitarbeitenden ab. Zu berücksichtigen sind hierbei auch mögliche Parallelbetriebe während der Übergangsphase sowie Aufwände für Change-Management und Kommunikation. Die Einzelheiten werden erst dem noch vorzulegenden Konzept zu entnehmen sein. Eine reine Gegenüberstellung zwischen den Lizenzkosten der bestehenden Anwendungen und den Microsoft 365 Lizenzen ist nicht ausreichend.
- Für die Kalkulation wird entscheidend sein, die vorhandenen und durch M365 evtl. ersetzbaren Anwendungen/Dienste zu ermitteln und hinsichtlich der Wirtschaftlichkeit der Ablösung zu analysieren.
- Auch der Aufwand für das regelmäßige Patchmanagement, Sicherheitsupdates und Versionsupgrades dürfte sich reduzieren, da diese Aufgaben im Cloudbetrieb weitgehend durch Microsoft übernommen werden.

2. *Das beauftragte Unternehmen stellt die entwickelte Strategie dem Werkausschuss vor und steht für Fragen zur Verfügung.*

Aktueller Sachstand hierzu:

Eine Informationsveranstaltung hierzu hat am 15.07.2025 stattgefunden.

3. *Die Verwaltung wird gebeten, ein Migrationsszenario zur Absicherung der Betriebsfähigkeit bei einem Wechsel auf alternative Lösungen und zur Absicherung eines ggf. notwendigen Wechsels auf eine onPremise-Lösung zu erarbeiten.*

Aktueller Sachstand hierzu:

Ein Exit aus Microsoft 365 erfordert eine strukturierte Vorgehensweise, um die Betriebsfähigkeit sicherzustellen. Zunächst sollten Alternativen zu M365 hinsichtlich Funktionalität, Sicherheit, Kosten und Kompatibilität evaluiert werden. Ein zentraler Aspekt ist die Datenmigration: Alle relevanten Inhalte wie E-Mails, Dokumente und Kalender müssen sicher und vollständig übertragen werden. Dabei ist auf geeignete Tools und die Integrität der Daten zu achten. Ebenso wichtig ist die Prüfung der Integration in bestehende Systeme und Prozesse, da M365 häufig tief eingebunden ist.

Die bestehenden Lizenzverträge sind auf dessen Laufzeit zu prüfen und individuelle Lösungen aus M365 sind zu identifizieren, die ggf. neu entwickelt werden müssen.

Im vorzulegenden Konzept werden die Themen M365 Exitstrategie, die damit zusammenhängenden Herausforderungen sowie mögliche Migrationswege explizit behandelt. Es muss beispielsweise im Rahmen einer Exitstrategie geprüft und berücksichtigt werden, wie sich der Wechsel auf andere integrierte Systeme und Arbeitsabläufe auswirken wird. Microsoft 365 ist eine umfassende Suite mit eng integrierten Anwendungen (wie Exchange Online, Microsoft Teams, SharePoint Online sowie OneDrive for Business). Eine neue Plattform könnte beispielsweise anders strukturiert sein oder einige Funktionen könnten fehlen, was die

Arbeitsabläufe beeinträchtigen würde. Wenn in Microsoft 365 maßgeschneiderte Lösungen oder Integrationen verwendet wurden, werden möglicherweise Entwicklungsressourcen benötigt, um äquivalente Funktionen auf der neuen Plattform zu implementieren.

Neben den oben genannten Sachständen zu der Beschlussvorlage 0027/2025 bietet Microsoft 365 nachstehende Vorteile, auch wenn diese zum jetzigen Zeitpunkt noch nicht abschließend qualifiziert werden können.

- a) Vorteile bzgl. Sicherheit, die in M365 enthalten sind
 - Mittels der Echtzeit-Bedrohungsanalyse werden Benutzer und Anmeldevorgänge in Echtzeit bewertet und die Risikovorgänge anhand von konfigurierten Richtlinien automatisch mitigiert.
 - Mittels der erweiterten Bedrohungserkennung auf den Endgeräten werden Verhaltensmuster analysiert und Angriffe in Echtzeit erkannt. Auf Bedrohungen wird automatisch reagiert und Gegenmaßnahmen werden eingeleitet.
 - Sollte, statt der bisherigen Software Sophos, der Defender *for Endpoint* (was noch geprüft werden muss, s. unter d)) genutzt werden, könnte dieser eine automatische Analyse und Inventarisierung von Endgeräten sowie der installierten Software durchführen. Dadurch würde das Inventar gegen aktuelle und vergangene Schwachstellen (CVSS) sowie Angriffsprofile geprüft und kategorisiert.
 - Falls eine Integration des Defender *for Identity* in die on-premises Active Directory erfolgt, würden verdächtige Aktivitäten wie Pass-the-Hash oder Reconnaissance in Echtzeit erkannt. Auch Angriffspfade, die zur Kompromittierung und Gesamtübernahme der Domäne führen können, würden analysiert und dargestellt.
- b) Moderner Arbeitsplatz
 - Kollaborative und interaktive Arbeit in Teams durch Chats, Video-Meetings, Dateiaustausch, Nutzung von kollaborationsorientierten Anwendungen wie Planner.
 - Gleichzeitiges gemeinsames und ortsunabhängiges Arbeiten an Dokumenten.
 - Zentrale Verteilung von Informationen und Dokumententemplates.
 - Die Versionierung von Dokumenten sowie die Nutzung von Metadaten (Autor, Erstelldatum, Dokumenttyp,) können in Prozessen und Automatisierungen (z.B. Power Automate Flows) zur Dokumentlenkung genutzt werden.
 - Über entsprechende Schnittstellen können aufbewahrungspflichtige Dokumente aus Microsoft 365 heraus (Microsoft Teams, SharePoint Online oder OneDrive for Business) in ein revisionssicheres Archiv wie d.velop d.3 archiviert werden. Die erforderlichen Funktionen hierzu stehen in den entsprechenden Lizenzen M365 E5 oder AddOn-Module M365 E5 EMS zur Verfügung.
 - Bei Bedarf können auch Zusammenarbeitsräume in Microsoft Teams für den sicheren Austausch von Dokumenten mit externen Partnern/Dienstleistern bereitgestellt werden. Die erforderlichen Funktionen (Microsoft Purview, Sensitivity Labels sowie weitere RMS- bzw. DLP-Funktionen) stehen in M365 zur Verfügung und können über die entsprechenden Lizenzen M365 E5 oder AddOn-Module M365 E5 EMS aktiviert werden. Somit kann zuverlässig verhindert werden, dass Dokumente außerhalb des M365 Tenants der KDZ gespeichert werden können.
- c) Weitere Vorteile gegenüber „herkömmlichem“ Windows & Office
 - Die Cloudversionen des Office Paketes (Microsoft 365 Apps for Enterprise) erhalten ständig neue Funktionen und Sicherheitsupdates. Somit ist sichergestellt, dass evtl. auftretende Sicherheitslücken oder Angriffsvektoren schnell und direkt durch den Hersteller geschlossen werden können.

- Daneben werden den Kunden automatisch immer die aktuellen Versionen bereitgestellt. Das heißt, die Unternehmenskunden müssen sich nicht mehr regelmäßig nach Ablauf des Supports neue App-Versionen kaufen und auf allen Geräten aktualisieren.
 - Die entsprechenden M365 Lizenzen können modular nach Bedarf bezogen werden und lassen sich flexibel skalieren. Neue Arbeitsplätze lassen sich so bedarfsgerecht hinzubuchen und ebenso wieder deaktivieren.
 - Bei der Zusammenarbeit mit externen Partnern (Gastusern) können diese M365 Services (wie Teams oder Sharepoint) mit ihren ggf. vorhandenen eigenen Lizenzen im M365 Tenant der Stadt Mainz nutzen.
- d) Betrachtung von Anwendungen, die potenziell durch M365-Produkte abgelöst werden könnten, und entsprechende Lizenzkosten einsparen könnten

Die KDZ Mainz hat in Zusammenarbeit mit der IT-Steuerung aktuell eingesetzte Anwendungen dahingehend untersucht, ob diese potenziell durch Anwendungen abgelöst werden könnten, die in M365 enthalten sind. Nachfolgend wird erläutert, um welche Anwendungen es sich handelt, welche jährlichen Lizenzkosten dafür derzeit anfallen und wie wahrscheinlich bzw. sinnvoll eine Ablösung dieser Anwendungen wäre. Vorab sei noch erwähnt, dass zwar noch weitere im Einsatz befindliche Anwendungen Einsparpotenziale (zugunsten M365) aufweisen, allerdings wird eine Ablösung hier (derzeit) nicht als zielführend betrachtet, weshalb sie in dieser Betrachtung nicht aufgeführt sind.

In diesem Dokument werden primär die Lizenzkosten betrachtet. Bei einer endgültigen Entscheidung über die hier aufgeführten Vorschläge, sind auch noch die zu erwartenden Migrations-, Betriebs- und Personalkosten zu berücksichtigen.

Die erste ablösbare Anwendung ist Cisco Webex. Diese könnte durch MS Teams ersetzt werden. Die Ablösung ist äußerst sinnvoll und realistisch und kann relativ unkompliziert erfolgen. Derzeit zahlt die Stadt Mainz ca. 21.000,- Euro Lizenzkosten für Webex. Demgegenüber würden mit der Umstellung auf M365 alle Mitarbeitende MS Teams nutzen können.

Die zweite Anwendung, die abgelöst werden kann und soll, ist HCL Notes. Hierbei ist jedoch zwischen dem Mailing-Teil und dem Teil „Datenbanken/Anwendungen“ zu unterscheiden. Der Mailing-Teil wird perspektivisch durch Exchange Online (Outlook) abgelöst werden. Demgegenüber müssen die vielen vorhandenen Datenbanken und Anwendungen durch verschiedene Produkte abgelöst werden, die nicht ausschließlich durch Microsoft-Produkte abzubilden sein werden. Die Lizenzkosten für HCL Notes betragen rund 223.000,- Euro. Bzgl. des Mailing-Teils sind Einsparungen möglich, da Exchange Online Teil der einzusetzenden M365-Lizenzen ist. Die Einsparungen bzgl. der Datenbanken und Anwendungen sind wiederum relativ zu betrachten, da noch nicht absehbar ist, ob hierzu ggf. weitere Drittanbieter-Software notwendig ist, die ihrerseits wieder Lizenzkosten verursachen könnte.

Citrix stellt die dritte theoretisch ablösbare Anwendung dar. Citrix unterteilt sich jedoch in verschiedene Anwendungsfälle, die unterschiedliche Ablöseszenarien zur Folge hätten. Bezieht man sich beispielsweise nur auf RDP, ist bereits weitgehend eine Ablösung durch Drittanbietersoftware erfolgt. Die Lizenzkosten hierfür belaufen/beliefen sich auf ca. 92.000,- Euro. Aufgrund der bereits teilweise erfolgten Ablösung ist das Einsparpotenzial diesbezüglich als gering zu bewerten.

Mit OpenText Advanced Authentication ist eine Software im Einsatz, die serverseitig als Basis einer Multifaktorauthentifizierung genutzt wird. Dies könnte unter Umständen ebenso durch eine entsprechende serverseitige Lösung der Fa. Microsoft erfolgen, was aber noch nicht abschließend geklärt ist. Die Lizenzkosten für OpenText Advanced Authentication liegen bei rund 32.000,- Euro, eine Ablösung, wenn machbar, ist relativ wahrscheinlich und sinnvoll, das Einsparpotenzial aufgrund der verhältnismäßig geringen Lizenzkosten jedoch ebenfalls nur gering.

Eine weitere Anwendung findet sich in Blackberry MDM, deren Lizenzkosten sich auf ca. 84.000,- Euro belaufen. Diese könnte theoretisch durch Microsoft Intune abgelöst werden. Allerdings existiert mit Matrix42 Silverback eine weitere Alternative, die ebenfalls kostenneutral (im Rahmen des bereits im Einsatz befindlichen Matrix42-Portfolios) genutzt werden könnte. Daher ist die Wahrscheinlichkeit der Ablösung von Blackberry MDM durch Microsoft Intune als eher gering zu bewerten.

Die nächste denkbare Anwendung ist EgoSecure FDE, die zur Festplattenverschlüsselung verwendet wird. Hierfür fallen derzeit Lizenzkosten i. H. v. 23.000,- Euro an. Die Funktionalitäten könnten durch Bitlocker übernommen werden. Die Wahrscheinlichkeit der Ablösung ist als hoch einzuschätzen, allerdings wäre eine Ablösung recht komplex, weshalb die Einsparung der relativ geringen Lizenzkosten eher langfristig zum Tragen käme.

Die Antivirensoftware Sophos könnte theoretisch durch Microsoft Defender for Endpoint ersetzt werden. Für Sophos sind Lizenzkosten von ca. 73.000,- Euro zu zahlen. Inwiefern Microsoft Defender jedoch vollumfänglich die Funktionalitäten von Sophos ersetzen kann, wird derzeit noch bewertet. Dies gilt auch für die Fragestellung, ob die Microsoft-Lizenzen auch den derzeit durch Sophos abgesicherten Server beinhalten. Insofern ist die Wahrscheinlichkeit einer Ablösung noch nicht abschließend beurteilbar.

Das städtische Intranet wird über die Contentmanagementsoftware von Sitepark realisiert. Das Intranet könnte theoretisch auch mittels Microsoft Sharepoint Online umgesetzt werden. Hierbei ist jedoch zu beachten, dass die Funktionalitäten des Systems von Sitepark vermutlich die von Sharepoint übersteigen, weshalb eine Ablösung weniger sinnvoll erscheint. Dies wird unterstrichen durch die sehr geringen Lizenzkosten und das damit geringe Einsparpotenzial für den Bereich Intranet i. H. v. ca. 2.500,- Euro.

Die KDZ Cloud (Filtr) wird zum einen für den Dateiaustausch mit Externen verwendet, zum anderen für den mobilen Zugriff auf Filr (via iOS); diese Bereiche sind insofern zu unterscheiden. Die Lizenzkosten für beides zusammen liegen bei ca. 21.000,- Euro. Ersetzt werden könnte die KDZ Cloud durch OneDrive, MS Teams sowie Sharepoint Online. Eine Ablösung ist möglich, jedoch mit einer gewissen Komplexität verbunden. Insofern ist das Einsparpotenzial (auch angesichts der genannten Lizenzkosten) eher gering.

Zuletzt käme noch die Anwendung 2Ask infrage, die als Umfragetool dient. Diese verursacht sehr geringe Lizenzkosten von rund 3.000,- Euro, allerdings existieren auch nur sehr wenige Benutzerkonten (weniger als 5). Mit Microsoft Forms könnte man diese Funktionalitäten ebenso abbilden. Ein Vorteil einer Ablösung von 2Ask durch MS Forms läge darin, dass damit alle User das Tool nutzen und Umfragen durchführen könnten (was auch die Nutzung von Online-Tools wie Doodle verringern dürfte). Insofern sind die

Einsparungen in Form von Lizenzkosten zum Status quo zwar gering, der spätere Mehrwert durch eine Ablösung wäre jedoch auf Nutzerseite gegeben.

Zu den Anwendungen, die bereits eingesetzt werden, treten noch weitere Anwendungen in der Betrachtung hinzu, die künftig eine Rolle spielen können/sollen.

So ist bereits jetzt Robotic Process Automation (RPA) ein erklärtes Ziel der Verwaltung. Da Microsoft 365 mit Power Apps/Power Automate bereits geeignete Anwendungen bereitstellt, würde man hier künftig Lizenzkosten sparen, da man für diese Zwecke keine weitere Drittanbietersoftware heranziehen müsste.

Gleiches gilt für Conceptboard, für das es bereits Anforderungen gibt. Dies könnte durch das Microsoft Whiteboard abgebildet werden und würde insofern ebenfalls künftige Einsparungen bringen, da eine Einführung kostenneutral (zumindest in Bezug auf Lizenzkosten) erfolgen könnte.

Es wird in Zukunft sicherlich noch eine Vielzahl weiterer Anwendungsfälle geben, die durch Produkte, die im M365-Portfolio enthalten sind, realisiert werden können und der Stadt Mainz insofern auch künftig zusätzliche Lizenzkosten ersparen könnten.

Nicht zu vergessen sind die nicht anfallenden Kosten für eine Neulizenzierung von Windows und Office, die sich auf jährlich ca. 831.000,- € belaufen würde.