NÜRNBERG

Moderner IT-Arbeitsplatz

auf Basis Microsoft M365



Dokumentinformationen

Erstellt von	IT/EA - MW
Datum Freigabe	15.03.2024
Freigabe durch	IT/L - AR
Klassifizierung[1]	SBK2

Dokumenthistorie

Version	Datum	Änderungen	Person
0.1	08.03.2024	Konzeptentwurf	IT/EA - MW
1.2	12.04.2024	Abstimmung mit ISB und DSB (09. & 12.04.2024)	ISB – US; ISB – SW; DSB – TD;
1.2	12.04.2024	DMS-Laufweg zur Schlusszeichnung IT/L, Genehmigung durch ISB, DSB Genehmigung durch Leitung Ref I/II	IT/L – AR; ISB – US; DSB – TB; Ref I/II - TB
1.3	18.09.2024	Einarbeitung Projektergebnisse	IT/L

Anmerkungen

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

[1] zur Klassifizierung wird verwiesen auf IS-RL-031/2020 im Intranet: https://intranet.stadt.nuernberg.de/imperia/md/zentral/dokumente/intranet/handbuch_der_verwaltung/vorschriften/0_buergermeisteramt_referate/hdv_020_62.pdf

Inhaltsverzeichnis

1. Management Summary 4

2. Ausgangsituation 5

2.1. Produktsuite Microsoft M365 6
2.2. Microsoft Office (O365) 6
2.3. Microsoft Teams 7
2.4. Gesamtbetrachtung 7
2.5. Cloud Identität & Multifaktor Authentifizierung 8
2.5.1. Cloud-Identität 8
2.5.2. Multifaktor-Authentifizierung (MFA) 8

3. Begründung für M365 9

3.1. M365 als strategische Plattform 9
3.2. Einsatz des De-Facto-Standards Microsoft Office mangels gleichwertiger Alternativen 9
3.3. Sicherstellung der Handlungsfähigkeit der Verwaltung und der Nutzerakzeptanz 10
3.4. Abbildung der IT-Security Anforderungen 10

4. Datenschutz und Informationssicherheit 11

5. Vorgehen zur Einführung von M365 in der Stadt Nürnberg 12

5.1. Phase 1 – Technischer Basisrollout M365 und Windows 11 12
5.1.1. Zeitraum 12
5.1.2. Inhalte 12
5.1.3. Beschreibung 12
5.2. Phase 2 – Einführung des modernen IT-Arbeitsplatzes auf Basis M365 13
5.2.1. Zeitraum 13
5.2.2. Inhalte 13
5.2.3. Beschreibung der einzelnen Produkte 13
5.2.3.1. Intune 13
5.2.3.2. Erweiterte MS Teams Funktionalität 14
5.2.3.3. Social Intranet auf Basis Microsoft Viva 14
5.2.3.4. Produktivitäts-Apps 15
5.2.3.5. Microsoft Defender 15
5.2.3.6. E5-Plan-Funktionalitäten 15
5.3. Phase 3 – Kontinuierliche Weiterentwicklung des modernen Arbeitsplatzes 17
5.3.1. Zeitraum 17
5.3.2. Inhalte 17
5.3.3. Beschreibung 17
5.3.3.1. Erweiterte Security Funktionen eines E5-Lizenzpaketes 17

6. Zyklische Überprüfung der Strategie 18

1. Management Summary

Die Stadt Nürnberg setzt aktuell die Microsoft Produkte Windows 10 Enterprise und Office 2016 auf den IT-Arbeitsplätzen in der Verwaltung ein. Ab Oktober 2025 stehen für diese Produkte keine Sicherheits- und Funktions-Updates mehr zur Verfügung. Ein weiterer Einsatz ist aus Gründen der Informationssicherheit nicht mehr möglich. Aktuell steht die Weiterentwicklung der ausschließlich lokal installierbaren Produkte seitens Microsoft noch in Frage. Darüber hinaus werden nur recht kurze Supportzeiträume garantiert, da Microsoft die Cloud-Varianten strategisch bevorzugt.

Der Fokus seitens Microsoft bzgl. deren Office Produkte liegt ab diesem Zeitpunkt ausschließlich auf den M365-Produkten mit Cloudanbindung zur Softwaremiete.

Es ist geplant, die Microsoft M365 Produktsuite als strategische Plattform in der Stadt Nürnberg einzuführen und gleichzeitig ein Upgrade des Windows Betriebssystems auf die Version 11 durchzuführen. Derzeit existiert keine vergleichbare Alternative zu dem Microsoft-Betriebssystem und Office-Produkten, welche die zukünftige Handlungsfähigkeit und Produktivität der Nürnberger Verwaltung in gleicher Form sicherstellt und unterstützt.

Die Einführung der Microsoft M365 Produktsuite erfolgt in drei Phasen:

Phase I

Technische Installation von Office 365 und Windows 11 bis Oktober 2025.

Phase II

Für eine bestmögliche Ausschöpfung der Funktionalitäten des Microsoft M365 / E3-Lizenzplans werden die enthaltenen Produkte in Bezug auf ihre Verwendbarkeit, den Datenschutz und die Informationssicherheit untersucht.

Ziel ist es einen modernen IT- Arbeitsplatz bis 2027 zu gestalten. Hierzu werden die im E3-Lizenzplan enthaltenen Produkte einzeln hinsichtlich Verwendbarkeit untersucht. Ein konkreter Einsatz ist erst nach Freigabe durch Datenschutz und Informationssicherheit möglich. Da alle diese Produkte cloudbasierend arbeiten, ist eine Einzelfallbetrachtung der Verwendung jedes Produktes erforderlich.

Phase III

Kontinuierliche Weiterentwicklung des modernen IT-Arbeitsplatzes, ggfls. mit individueller Prüfung der Lizenzierung eines E5-Lizenzplanes.

Dieses Dokument beschreibt die derzeitige Ausgangssituation, begründet den Handlungsbedarf und die Notwendigkeit sowie das Fehlen von Alternativen zur Einführung von Microsoft M365.

Weiterhin wird das dreistufige Projektvorgehen im Rahmen des Gesamtprogrammes erläutert.

Vorteile, Synergieeffekte und Einsatzmöglichkeiten der Einführung der M365-Plattform in der Stadtverwaltung der Stadt Nürnberg werden erklärt.

2. Ausgangsituation

Die Stadtverwaltung Nürnberg setzt im **Bereich der Büroarbeitsplätze** seit Mitte der 90er-Jahre diverse Microsoft-Produkte ein.

Im Betriebssystembereich beginnend mit dem 16-Bit-Betriebssystem MS Windows 3.1 auf Einzelplätzen und mit MS Windows für Workgroups 3.11 für die erste Vernetzung von PCs in lokalen Arbeitsgruppen. Seitdem wurde mit wenigen Ausnahmen (z. B. wurde MS Windows Vista übersprungen) die jeweilige Nachfolgeversion des Windows-Betriebssystems flächendeckend eingesetzt. Alternative Betriebssysteme wie beispielsweise Linux, MacOS oder OS/2 konnten nie eine ausreichende Verbreitung und Unterstützung im Softwaremarkt erreichen, um die vielfältigen Anforderungen einer Großstadtverwaltung abdecken zu können.

Ähnlich verhält es sich im **Bereich der Office-Produkte**.

Auch hier hat die Stadt Nürnberg schon Mitte der 90er-Jahre die Microsoft-Produktpalette eingesetzt. Die ursprünglich eingesetzten Einzelprodukte wie MS Word 2.0 und MS Excel 4.0 wurden in der Folge durch die in Office-Paketen gebündelten Versionen MS Office 4.2 und 4.3 ersetzt. Der Einsatz von MS Office-Paketen hat neben finanziellen Aspekten (der Kauf der Einzelprodukte war in der Summe teurer) auch einen Mehrwert im Zusammenspiel der Produkte erbracht, da schon damals die Produkte mit innovativen Techniken wie DDE[2] oder auch OLE 2.0 aufwarten konnten und die Produktpalette (Word, Excel, PowerPoint, Access) in der Breite die Office-Bedarfe gut abdecken konnte.

Mit der Markteinführung von MS Outlook 1997 hat sich die Marktposition nochmals verstärkt und die Microsoft Office-Palette bildete den De-Facto-Standard im Bereich der Office-Produkte. Auch hier konnten alternative Angebote, z. B. von den Firmen Lotus oder IBM oder auch Open-Office, nicht die notwendige Marktdurchdringung erreichen, um eine umfassende Unterstützung im Fachverfahrensbereich zu erlangen. In der Folge wurden jeweils Nachfolgeversionen der MS Office-Produktpalette in der Stadtverwaltung eingesetzt.

Die Kontinuität im PC-Betriebssystembereich und bei den Office-Produkten hat dazu geführt, dass sowohl die Administrations- und Support- als auch die Schulungsaufwände aufgrund dieser Standardisierung minimiert wurden. Die breite Unterstützung bzw. Angebote anderer Softwarehersteller, insbesondere der für die Stadt Nürnberg wichtige Fachverfahrensbereich, hat sichergestellt, dass sowohl das Angebot notwendiger Fachverfahren als auch die Zukunftsfähigkeit der Lösungen ausreichend gegeben waren.

Die Stadt Nürnberg setzt derzeit Windows 10 Enterprise und MS Office 2016 (Standard und Professional) ein. Beide Produkte sind am Ende ihres Produktlebenszyklus, das End of Life (EOL) ist der 14.10.2025. Danach sind für beide Produkte keine Sicherheitsupdates mehr verfügbar und ein Weiterbetrieb stellt somit ein Sicherheitsrisiko dar. Es besteht daher dringender Handlungsbedarf, beide Produkte bis zu diesem Datum zu ersetzen.

[2] DDE: Abkürzung des englischen Begriffs „Dynamic Data Exchange“, ist ein Protokoll für den Datenaustausch zwischen verschiedenen Anwendungen

2.1. Produktsuite Microsoft M365

Microsoft bezeichnet mit M365 eine Software-Produktfamilie, die aus den **drei Hauptkomponenten**

- Office 365 (O365),
- Enterprise Mobility Suite (EMS365) und
- Windows Enterprise Betriebssystem (Windows 11 Enterprise) besteht.

Diese drei Hauptkomponenten werden jeweils einzeln, oder nach Funktionsumfang abgestuft zusammen in einem sogenannten **E1/E3/E5-Lizenzplan** mit zeitlich begrenztem Nutzungsrecht zur Softwaremiete (Subscription) pro Benutzer angeboten.
Ein Erwerb von dauerhaften M365 Nutzungsrechten (Kauflizenzen) und die Lizenzierung einzelner Endgeräte sind nicht mehr vorgesehen.

Die erste **Komponente Office 365 (O365)** umfasst neben den Standard Office Applikationen (Word, Excel, PowerPoint, Outlook) auch eine Reihe weiterer Produktivitäts-Apps für verschiedene Einsatzzwecke (z.B. wie OneNote[3], Planner[4], Viva[5] u.a.). Bis zu einem EU-Urteil zur Entkoppelung von MS Teams und MS Office war auch MS Teams Bestandteil von MS Office 365.

Die zweite Komponente **Enterprise Mobility Suite** (EMS365) beinhaltet neben der Cloud-Benutzerverwaltung Entra-ID hauptsächlich administrative und technische Funktionalitäten, wie beispielsweise Microsoft Intune für die Softwareinstallation auf Endgeräten.

Die dritte Komponente der M365 Suite umfasst das Recht, immer die **aktuelle Version** des Client Betriebssystems Windows einzusetzen, aktuell Windows 11 Enterprise sowie unterstützende, administrative Tools im Bereich des Client Betriebssystems.

Flankierend dazu, beinhaltet M365 in den verschiedenen E-Plänen erweiterte Funktionalitäten in den Bereichen IT-Security (z.B. den Virenscanner Microsoft Defender), Compliance und Telefonie bzw. Kommunikation.

Ebenfalls Bestandteil eines E-Planes sind die Cloud-Dienste SharePoint Online und Exchange Online, auf deren Basis die Dateispeicherung und das Versenden von E-Mails in der Cloud erfolgen kann. Dies ist möglich, ohne Server im eigenen Netzwerk für diese Dienste bereitstellen zu müssen. Es ist allerdings genau zu prüfen, ob die Speicherung in der Cloud aus Sicht des Datenschutzes und der Informationssicherheit überhaupt zulässig ist.

Eine Übersicht der Einzelkomponenten von M365 ist unter folgendem Link zu finden: https://m365maps.com/files/Microsoft-365-Enterprise-All.htm

2.2. Microsoft Office (O365)

Das derzeit eingesetzte MS Office 2016 wurde als reine Kaufversion erworben. Ein Update-Recht auf eine aktuelle MS Office Version ist damit nicht verbunden, so dass eine komplette Neulizenzierung notwendig ist.

Im Office-Bereich hat Microsoft schon seit einiger Zeit den Schwerpunkt auf die Cloud-Produkte O365/M365 gelegt. Das letzte veröffentlichte reine OnPrem[6]-Office ist die Version 2021 mit End-of-

[3] **Microsoft OneNote** ist eine digitale Notizen-App, die einen zentralen Ort zum Aufbewahren all Ihrer Notizen, Recherchen, Pläne und Informationen bietet
[4] Microsoft Planner ist eine Kanban-Lösung, die einfache Aufgabenverwaltung und To-do-Listen für die Teamarbeit bietet
[5] **Microsoft Viva** ist die Plattform für Mitarbeitererfahrung in Microsoft 365 und Teams.
[6] OnPrem: Abkürzung des englischen Begriffs „on premise“, das heißt lokal, auf dem eigenen PC oder Server, installiert

live (EOL[7]) am 13.10.26. MS Office 2024 wurde Anfang April 2024 angekündigt, eine Veröffentlichung ist für Oktober 2024 vorgesehen. Damit ist es mit den notwendigen Vorarbeiten faktisch nicht mehr möglich, diese Version bei der Stadt Nürnberg bis zum Oktober 2025 als Nachfolgeversion auszurollen. Wie lange diese Version unterstützt wird ist ebenfalls noch offen. Aufgrund der Versionspolitik von Microsoft in den letzten Jahren ist mit einem relativ kurzen Supportzeitraum zu rechnen.. Die **Zukunftsfähigkeit** von reinen OnPrem-Office-Varianten ist insgesamt kritisch zu betrachten, da Microsoft - wie viele andere Softwarehersteller - seine Produkte zukünftig nur noch cloudbasiert anbietet.

Aktive Produktentwicklung und die **Integration von Innovationen** (z. B. KI) sind vor allem für die Online-Versionen zu erwarten. Diese werden mehr und mehr auch die Basis von darauf aufsetzenden weiteren Produkten anderer Hersteller sein (z.B.: Bereich Social Intranet etliche Produkten MS VIVA (die Social Intranet App von Microsoft).

Die Marktdurchdringung der Microsoft-Produkte und die damit erreichte Position als De-Facto-Standard, hat auch dazu geführt, dass die von **Microsoft verwendeten Dokumentenformate** einen De-Facto-Standard darstellen. Der Dokumentenaustausch und die Dokumentenbearbeitung mit externen Stellen gestaltet sich mit den Dokumentenformaten von Microsoft (z. B. .docx, .xlsx usw.) zumeist unproblematisch, da auch bei den Kommunikationspartnern größtenteils MS Office-Produkte eingesetzt werden. Kompatibilitätsprobleme treten hier im Gegensatz zur Verwendung anderer Formate im Regelfall nicht auf.

Es sind weiterhin viele bei der Stadt Nürnberg eingesetzte Anwendungen auf eine MS Office-Version angewiesen bzw. können nur eingeschränkt Alternativen wie Libre-/Open Office unterstützen („Anhang MS-Office relevante Anwendungen“).

2.3. Microsoft Teams

Derzeit wird MS Teams als Chat- und Audio-/Video-Tool eingesetzt. MS Teams ist eine umfassende **Kollaborations-Plattform**, die aus datenschutzrechtlichen Gründen nur mit einigen Grundfunktionen eingesetzt wird.

Aufgrund von Vorgaben der EU ist MS Teams seit 01.10.23 standardmäßig nicht mehr in den von Microsoft angebotenen Enterprise Plänen (E1-E5) enthalten. Das Lizenzmanagement des Amts für Informationstechnologie konnte durch die vorsorgliche Beschaffung von einzelnen Lizenzen für die Stadt Nürnberg sicherstellen, dass MS Teams trotzdem ohne weitere Mehrkosten als „Altkunde“ in den Enterprise Plänen inkludiert ist.

In Phase 2 wird geprüft, ob eine erweiterte Funktionalität von MS Teams freigegeben werden kann. Mittlerweile gibt es für MS Teams ein zusätzlich zu lizenzierendes Add-On (MS Teams Premium), welches weitere für die Stadt Nürnberg interessante Funktionalitäten bietet. Vor allem die mit diesem Add-On nutzbare Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmern einer Audio-/ Videokonferenz ist ein Feature, welches bei sensiblen Gesprächsinhalten Vorteile hat. Zur Nutzung dieses Features benötigt lediglich der Besprechungsorganisator eine Add-On Lizenz MS Teams Premium.

2.4. Gesamtbetrachtung

Derzeit ist ein Verzicht auf ein MS Windows Betriebssystem und auf eine aktuelle MS Office-Variante nicht realistisch umsetzbar.

[7] EOL: Abkürzung des englischen Begriffs „End of Life“, der so viel bedeutet wie Produktlebensende

Die Anforderungen von Seiten der fachlich notwendigen Programme setzen immer noch zu einem überwiegenden Teil den Einsatz der Microsoft Produkte voraus, diese gelten in vielen Bereichen (Schnittstellen, Dokumentformate) als De-Facto-Standard.

2.5. Cloud Identität & Multifaktor Authentifizierung

2.5.1. Cloud-Identität

Um die steigende Anforderungen der Stadtverwaltung nach modernen Anwendungen und Funktionalitäten erfüllen zu können ist es notwendig, vermehrt Cloud-Anwendungen einzusetzen.

Diese Anwendungen werden mit einer unabhängigen Benutzerverwaltung betrieben, so dass die Anwender dafür einen separaten Benutzernamen mit Kennwort verwenden müssen. Dies führt dazu, dass mehrere Anmeldevorgänge notwendig sind, die Benutzerfreundlichkeit leidet und der Administrationsaufwand entsprechend erhöht ist.

Die meisten SaaS-Anwendungen[8] bieten die Möglichkeit eine Cloud-Identität zu verwenden. Über ein einheitliches Benutzerkonto kann man sich in der Praxis bei mehreren Anwendungen einheitlich anmelden.

Microsoft bietet mit der **Entra-ID eine derartige Cloudidentität** an, die zum einen einfach mit dem schon vorhandenen Benutzerverzeichnis Active Directory Services koppelbar ist und zum anderen eine breite Unterstützung durch die verschiedenen Software-as-a-Service-Anbieter (SaaS) erfährt.

2.5.2. Multifaktor-Authentifizierung (MFA)

Erhöhte **Datenschutz- und Informationssicherheitsanforderungen** erfordern die Implementierung einer Multifaktor-Authentifizierung (MFA) bei der Anmeldung am Rechner. Zur Benutzung werden zwei unabhängige Faktoren eingesetzt (z. B. Passwort und Zertifikat auf einer Smartcard).

Die Einführung von MFA ist unter anderem eine Forderung der Informationssicherheit und des Datenschutzes und eine Voraussetzung für den **Erhalt von Fördergeldern im Rahmen des DiGIN-Projekts** des Gesundheitsamtes (Gh).

Bei der zeitlich kritischen und notwendigen Einführung für MFA bei Gh sollte die gleiche Softwarelösung verwendet werden, wie später für alle städtischen User. Die bevorzugte Lösung von Microsoft deckt am besten die vorhandenen Anforderungen der Stadt Nürnberg ab.

Die Integration einer MFA in die oben beschriebene Lösung mit Microsoft-Cloud-Identität (Entra-ID) ist hier ebenfalls problemlos möglich, sodass das **Sicherheitsniveau entschieden verbessert** wird und gleichzeitig die **Benutzerfreundlichkeit steigt**.

[8] SaaS - Software as a Service: Ist ein cloudbasiertes Softwaremodell, das Anwendungen über einen Internetbrowser an Endbenutzer liefert.

3. Begründung für M365

3.1. M365 als strategische Plattform

Der in der Vergangenheit genutzte Ansatz sah für jede Problemstellung die Auswahl der bestmöglichen Softwarelösung vor. Dadurch wurden viele hochspezialisierte Softwareprodukte eingesetzt, die zwar ihre Aufgaben zielgenau lösen, aber keine oder wenig Interaktion mit anderen Systemen vorsehen bzw. deren Gesamtintegration sehr aufwändig und ressourcenintensiv ist.

Der **integrierte Plattformansatz** von Microsoft M365, bei dem die eingesetzten Softwareprodukte **nahtlos interagieren**, schafft hier Abhilfe, um die Komplexität der IT-Landschaft zu reduzieren, Prozesse zu automatisieren und zu digitalisieren.

3.2. Einsatz des De-Facto-Standards Microsoft Office mangels gleichwertiger Alternativen

Aktuell existiert keine gleichwertige Alternative zur Microsoft Office Plattform, die alltagstagstauglich eingesetzt werden kann. Microsoft definiert mit seinen Produkten derzeit den De-Facto-Standard im Office- und Kollaborationsbereich.

Ebenso ist ein Verzicht auf das Betriebssystem MS Windows aufgrund der Anforderungen der bei der Stadt eingesetzten Fachverfahren nicht möglich. Bei einer Stichprobe von über 50 Prozent der derzeit eingesetzten Fachverfahren, Schnittstellen und Hilfstools wurden über 75 identifiziert, die derzeit nur mit MS Office Produkten kompatibel sind. („Anhang MS-Office relevante Anwendungen“). Gleichzeitig steigt aufgrund der **fortschreitenden Digitalisierung** der **Bedarf an einer modernen Bürosoftware**. Neben einer möglichst eingängigen bzw. bekannten Bedienung wird auch das **Zusammenspiel mehrerer Programme und Komponenten** immer wichtiger, um möglichst effizient und schnittstellenarm arbeiten zu können.

Im Wettbewerb um **qualifiziertes Fachpersonal** wird es immer wichtiger, eine zukunftsfähige Umgebung anzubieten, die neben modernen Funktionalitäten auch das mobile Arbeiten unterstützt.

Die Microsoft M365-Plattform bietet in der Summe hier die größten Vorteile. Die M365-Plattform von Microsoft zeichnet sich durch eine umfangreiche App-Palette für den Einsatz im Office-Umfeld aus, die gut aufeinander abgestimmt und nahtlos integriert ist, eine einheitliche Administration ermöglicht und eine hohe Innovationsgeschwindigkeit zeigt.

Mit dem **KI-Assistenten „Copilot“** ist es Microsoft gelungen, sehr frühzeitig das Thema künstliche Intelligenz in den Office-Bereich zu integrieren. Aufgrund der Marktdominanz des De-Facto-Standards ist außerdem zu erwarten, dass auch weiterhin die bei der Stadt eingesetzten Fachverfahren eine Kompatibilität mit den Microsoft-Produkten bereitstellen.

Alternative Produkte (z.B.: Libre Office, Collabora, etc.) bieten hingegen entweder nur Teile des Leistungsspektrums ab oder bieten nicht die notwendige Kompatibilität mit den bei der Stadt im Einsatz befindlichen Fachverfahren.

Der von kommunalen Dienstleistern entwickelte digitale Arbeitsplatz „dPhoenix Suite“ kommt zum gegenwärtigen Zeitpunkt sowohl aus Effizienzgründen als auch im Hinblick auf notwendige **Migrationskosten und fehlende Integrationsmöglichkeiten** in bestehende Fachverfahren derzeit nicht in Betracht.

Dies gilt auch für **alternative Cloud-Plattformen** wie z.B. Google Workplace. Google hat eine Cloud-Suite geschaffen, die die grundsätzlich notwendigen Funktionalitäten (Textverarbeitung, Tabellenkalkulation usw.) abdeckt. Google ist in der Cloud-Orientierung noch einen Schritt weiter, da diese Apps nur noch in einer Online-Variante existieren. Eine lokal installierbare Office Suite ist nicht verfügbar, die Abhängigkeit von einer Internetverbindung damit fast vollständig gegeben. Zudem sind Schnittstellen von Fachverfahren zu diesen Produkten eher eine Seltenheit.

3.3. Sicherstellung der Handlungsfähigkeit der Verwaltung und der Nutzerakzeptanz

Die **Funktionsfähigkeit von Fachverfahren** und damit die Handlungsfähigkeit der Verwaltung – gerade in Bezug auf die Integration eines Office Produktes in die vielfältigen Fachverfahren – hat eine sehr hohe Priorität.

Weiterhin bieten die Produkte europäischer Hersteller zum gegenwärtigen Zeitpunkt nicht die Benutzer-Akzeptanz **und die Kompatibilität** wie die Microsoft Plattformprodukte und würden somit durch die Umstellung zu einem höheren Aufwand für die städtischen Dienststellen und Betriebe führen.

Die Nutzung cloudbasierter Dienste führt zu einer **Entlastung der gesamtstädtischen Informationstechnologie**, die derzeit mit einem Anteil von ca. 15-20 Prozent nicht besetzter Stellen in einem von Fachkräftemangel geprägten Arbeitsmarkt dringend entlastende Technologien benötigt.

Nur so ist die Funktionsfähigkeit der IT der Stadtverwaltung, bei den aufgrund der Digitalisierung steigenden Anforderungen, zu gewährleisten.

3.4. Abbildung der IT-Security Anforderungen

In der Microsoft M365 sind IT-Security-Funktionen abgedeckt, die Mehrwerte und Synergien in der Administration bieten, hierdurch können einige bereits aktuell lizenzierte Produkte anderer Hersteller ersetzt werden.

4. Datenschutz und Informationssicherheit

Der Einsatz von M365-Produkten wurde hinsichtlich des Datenschutzes zunächst sehr kritisch gesehen. Einer der Hauptkritikpunkte war der mögliche Datenabfluss in Drittländer mit nicht ausreichendem Datenschutzstandard aufgrund der Cloud-Standorte von Microsoft. Mittlerweile hat sowohl Microsoft einige Verbesserung herbeigeführt als auch die rechtliche Lage eine Änderung erfahren.

Zur Minimierung dieser berechtigten Kritikpunkte hat Microsoft die sogenannte EU-Datengrenze ("**EU Data Boundary Services**") eingeführt, nach der eine Datenverarbeitung in den Rechenzentren der EU und ansonsten eine Pseudonymisierung[9] von Protokolldaten erfolgt[10]. Die EU-Datengrenze ist im Rahmen des Einsatzes von M365 gewährleistet.

Seit 10.07.2023 existiert ein **Angemessenheitsbeschluss der EU** für das EU-U.S. Data Privacy Framework[11]. Dies bedeutet, dass unter den Bedingungen dieses Frameworks der USA hinsichtlich des Datenschutzes ein angemessenes Datenschutzniveau attestiert wird. Die Firma Microsoft ist ein im Sinne dieses Frameworks zertifiziertes Unternehmen[12].

Hinsichtlich der Verwendung von MS Teams wurde vielfach die fehlende **Ende-zu-Ende-Verschlüsselung** (End-to-End-Encryption - E2EE) bei Kommunikation mit mehreren Teilnehmern kritisiert. Mittlerweile bietet Microsoft ein AddOn für MS Teams (MS Teams Premium) an, welches erweiterte Funktionen bietet. Unter anderem ist es dadurch möglich, eine Ende-zu-Ende-Verschlüsselung auch bei mehreren Teilnehmern zu aktivieren, so dass eine unbeabsichtigte Kenntnisnahme der Audio-/Videoübertragungen im Übertragungsweg verhindert wird[13].

Microsoft Cloud-Produkte sind somit umfangreich nach Informationssicherheitsstandards zertifiziert[14]. Unter anderem liegt für das in M365 enthaltene Office 365 (O365) eine **ISO 27001-Zertifizierung** vor. Zusätzlich werden die **Anforderungen nach dem Cloud Computing Compliance Criteria Catalog** (C5) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllt[15].

In der Summe erscheint der Einsatz von M365 im angedachten Rahmen voraussichtlich vertretbar.

Dennoch ist aufgrund der großen Anzahl der über M365 verarbeiteten bzw. generierten personenbezogenen Daten (Nutzungsdaten, erstellte Dokumente etc.) sowie der teilweisen Nutzung neuer Technologien (z. B. Copilot) verpflichtend eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, um die mit dem Einsatz von M365 verbundenen Risiken aufzeigen und bewerten sowie hieraus erforderliche technische und organisatorische Maßnahmen zur Risikominimierung ableiten und implementieren zu können. Das danach verbleibende Restrisiko ist dann ebenfalls zu bewerten und muss dann letztlich von der Verwaltungsspitze getragen werden. Die DSFA hat hierbei sämtliche zur Nutzung vorgesehene Funktionen und Apps zu umfassen, wobei die DSFA im Rahmen der nachträglichen Hinzunahme weiterer Funktionen/Apps auch entsprechend erweitert werden kann.

[9] Bei der Pseudonymisierung werden personenbezogene Daten (meist Namen) durch Codes oder Identifikationsnummern ersetzt
[10] siehe https://learn.microsoft.com/de-de/privacy/eudb/eu-data-boundary-learn
[11] siehe https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en
[12] siehe https://www.dataprivacyframework.gov/list
[13] siehe https://learn.microsoft.com/de-de/MicrosoftTeams/enhanced-teams-experience
[14] siehe Complianceangebote für Microsoft 365, Azure und andere Microsoft-Dienste. | Microsoft Learn
[15] siehe https://learn.microsoft.com/en-us/compliance/regulatory/offering-c5-germany

5. Vorgehen zur Einführung von M365 in der Stadt Nürnberg

5.1. Phase 1 – Technischer Basisrollout M365 und Windows 11

5.1.1. Zeitraum

Die Phase 1 erstreckt sich bis zum Oktober 2025.

5.1.2. Inhalte

- Einrichtung des Microsoft Cloud Tenants (Grundstruktur)
- Einrichtung der Entra-ID und Vorbereitung der Multifaktor-Authentifizierung
- Vorbereiten und Testen der Windows 11 Installation
- Vorbereiten und Testen Office 365 Installation inkl. MS Teams
- Stadtweiter Rollout von Windows 11 und Office 365 (kombiniert)

5.1.3. Beschreibung

Das **Ende des Supportzeitraums** von MS Windows 10 Enterprise und MS Office 2016 (Standard und Professional) zum 14.10.2025 (Ende der Sicherheitsupdates) macht es notwendig, diese beiden Produkte vordringlich abzulösen, um die Funktionsfähigkeit der Stadtverwaltung und die IT-Sicherheitsstandards durch Einsatz aktuell gepatchter Softwareprodukte weiterhin sicherzustellen.

Aufgrund der noch zur Verfügung stehenden Zeit und der vorhandenen personellen Ressourcen ist eine Fokussierung auf die Ablösung dieser Produkte zwingend notwendig. Die neue Betriebssystemversion MS Windows 11 Enterprise ist bereits über den vorhandenen Rahmenvertrag Microsoft Enterprise Agreement lizenziert.

Als Einstieg in die strategische M365-Plattform wird MS Office (O365) weiterhin lokal auf den Endgeräten installiert. Die lokale Installation von O365 setzt für die Installation, Aktivierung und Lizenzierung in allen Lizenzformen immer ein Microsoft Cloud-Benutzerkonto in der Entra-ID voraus.

Microsoft Teams wird dieser Phase im derzeitigen Umfang betrieben, um die bisher darauf basierende Kommunikation und die Arbeit im Homeoffice sowie das mobile Arbeiten unterbrechungsfrei weiter unterstützen zu können. MS Teams kann in dieser Phase weiterhin ausschließlich für die Audio- bzw. Videokommunikation, Chat und Bildschirm Sharing genutzt werden.

Zur Ermöglichung der O365-Installation und zur Erfüllung der bestehenden Anforderungen an eine Cloud-Identität (s.o.) und eine Multifaktor-Authentifizierung muss die MS Entra-ID im Rahmen dieses Projekts implementiert werden. Dabei wird die bisherige lokale städtische Benutzerverwaltung (Microsoft Active Directory) mit der Entra-ID (also mit der Benutzerverwaltung in der Cloud) synchronisiert.

In enger Abstimmung mit dem Datenschutz werden nach dem Minimalprinzip nur die minimal erforderlichen Benutzerkonten- und Endgeräteinformationen in die Entra-ID übertragen. Die Übermittlung von Telemetrie- und Protokolldaten an Microsoft wird soweit technisch möglich unterbunden und nur in begründeten Einzelfällen (z.B. Aufrechterhaltung der IT-Sicherheit) zugelassen.

Nach der Konfiguration und Testen der Office 365 und Windows 11 Enterprise Installationen erfolgt der sukzessive Rollout für alle User bis Ende Oktober 2025.

5.2. Phase 2 – Einführung des modernen IT-Arbeitsplatzes auf Basis M365

5.2.1. Zeitraum

Die Programmphase 2 startet ab November 2025 und erstreckt sich nach derzeitiger Planung über einen Zeitraum von circa 2 Jahren.

5.2.2. Inhalte

Soweit nach Prüfung durch Informationssicherheit, Datenschutz und Personalvertretung ein Einsatz ermöglicht werden kann, sollen folgende Produkte der M365-Suite zur Nutzung untersucht werden:

- Microsoft Intune für die endgeräteübergreifende Softwareinstallation und -konfiguration, Ersatz der bisherigen Drittanbieterlösung
- Erweiterte Funktionalität von MS Teams sowie von MS Teams Premium, soweit erforderlich; in diesem Zusammenhang auch Regelung und Prüfung der Zulässigkeit einer Datenablage in der Cloud
- Social Intranet auf Basis Microsoft Viva (vorbehaltlich der Entscheidung von KoM für Viva)
- Weitere im E3-Plan enthaltene Produktivitäts-Apps (Power Apps, Power Automate, Planner) und Online-Dienste (SharePoint Online, Exchange Online)
- Endpoint-Security (Virenschutz) auf Basis Defender
- Funktionalitäten, die im Rahmen eines Upgrades auf einen E5-Plan zur Verfügung stehen würden

5.2.3. Beschreibung der einzelnen Produkte

Aufbauend auf die Arbeiten der Phase 1 (technischer Basis-Rollout M365), werden in Phase 2 zusätzliche im E3-Plan enthaltene Funktionen und Apps aktiviert, soweit diese benötigt werden und seitens ISB und DSB freigegeben werden können.

5.2.3.1. Intune

Der technische M365-Basisrollout erfolgt mit der existierenden Softwareverteilung Empirum für PCs, Laptops und einer Lösung der Firma VMWare für mobile Geräte.

In Phase 2 sollen diese beiden Produkte sodann vollständig durch das Produkt Microsoft Intune abgelöst werden.

Die aktuelle **Softwareverteilung benötigt derzeit 2 Lösungen** für PCs/Laptops und mobile Geräte (iPhone, iPad) und soll zukünftig nur noch von einer zentralen Lösung (MS Intune) gesteuert werden.

Dies führt zu Einsparungen im Bereich der Lizenzierung der bisherigen Produkte und reduziert den Personaleinsatz bei gleichzeitiger Erhöhung der IT Sicherheitsstandards (aufgrund der einheitlichen Administration aller Endgeräte).

Intune bietet die Möglichkeit, sowohl klassische Software (Programme) als auch Windows Apps auf den Endgeräten zu installieren, zu aktualisieren oder auch zu entfernen (unerwünschte Programme).

Die Installation kann dabei sowohl verpflichtend (zentral über die IT) als auch vom Anwender aus einem Software-Kiosk vorgenommen werden. Endgeräte werden nicht mehr vorkonfiguriert, sondern

direkt vom Anwender nach dem Auspacken eingerichtet. Über einen Self Service sind die Mitarbeiter in der Lage, Probleme ohne Inanspruchnahme der IT-Hotline zu bewältigen.

Weiterhin kann Intune Endgeräte mit Windows-Updates und vorgelagerten Test-Bereichen versorgen. Dabei können die Clients automatisiert auf Konformitätsregeln überprüft und entsprechend behandelt werden.

Zentrale, vereinheitlichte Übersichten stellen in vielen Bereichen eine Zusammenfassung der Client-Status-Informationen zur Verfügung und die zentrale IT wird unterstützt, lokal genutzte Einstellungen in die Cloud-Verwaltung zu überführen (z.B. Gruppenrichtlinien, usw.).

5.2.3.2. Erweiterte MS Teams Funktionalität

MS Teams wird seit Einführung als Videoplattform mit Chat- und Bildschirmteilungs-Funktion eingesetzt. Alle erweiterten Funktionalitäten von MS Teams wurden soweit möglich deaktiviert.

In Phase 2 soll nach Prüfung durch Datenschutz und Informationssicherheit die Freischaltung der erweiterten Funktionen von MS Teams erfolgen. MS Teams soll damit von der reinen **Videokommunikationsplattform zur Kollaborationsplattform** ausgebaut werden. Es soll die **Integration in Office** (Kalender, Kontakte) erfolgen und nach Bedarf sollen auch zusätzliche Besprechungsfunktionen von MS Teams Premium aktiviert werden. Weiterhin sollen die Ablage und der Austausch von Dateien und Inhalten über den Cloud-Dienst SharePoint-Online geprüft und gegeben falls freigegeben werden.

Ziel ist die Einführung des **modernen IT-Verwaltungs-Arbeitsplatzes** auf Basis MS Teams, in dem alle Kommunikationskanäle (Videokommunikation, Chat, Messenger, E-Mail) gebündelt werden und die Office 365 Produktivitäts-Apps für das effektive Zusammenarbeiten zur Verfügung stehen.

5.2.3.3. Social Intranet auf Basis Microsoft Viva

Unter der Annahme, dass die Entscheidung des Projektteams des Amtes für Kommunikation und Stadtmarketing für die im E3-Plan enthaltene **Microsoft Viva Suite** fällt, soll ein Rollout des neuen Social Intranets auf Basis dieser Produkte erfolgen.

Das Social Intranet auf Basis Viva ermöglicht **dienststellenübergreifende Social Media Kommunikationsformen** innerhalb der Stadt Nürnberg und ist dabei gleichzeitig voll in die M365-Welt integriert.

Die **Berechtigungssteuerung** erfolgt zentral über die Entra-ID und bezieht dabei auch Non-Desktop-Worker ohne eigenes städtisches Endgerät mit ein, die über vergünstigte M365-Lizenzen auf die Inhalte des Social Intranets zugreifen können.

Das Social Intranet auf Basis Viva ist somit vollständig in den modernen IT-Verwaltungs-Arbeitsplatz integriert und ergänzt die Zusammenarbeit um moderne Formen der innerstädtischen Kommunikation.

5.2.3.4. Produktivitäts-Apps

Neben den **klassischen Office Produkten** (Word, Excel, PowerPoint, OneNote und Outlook) enthält der M365 E3-Plan eine Reihe von weiteren Produktivitäts-Apps, die sich nahtlos in die M365-Welt integrieren.

Die folgende Aufzählung stellt einen Auszug einiger der wichtigsten Produktivitäts-Apps dar:

- **Power-Apps**
  Power Apps bieten die Möglichkeit, ohne Programmierkenntnisse selbst kleine Anwendungen zu erstellen – dies wird auch Low Code / No Code Entwicklung bezeichnet.
- **Power Automate**
  Power Automate ist die RPA-Lösung (Robotic Process Automation) im Kontext von M365. Derzeit setzt die Stadt Nürnberg im RPA-Umfeld auf das Produkt UI-Path ein. In Phase 2 wird überprüft, inwieweit Power Automate ergänzend oder substituierend zu UI Path zum Einsatz kommen kann.
- **Planner**
  Planner ermöglicht eine Aufgabenplanung in Kanban-Boards mit ergänzenden Dateien, Checklisten und Bezeichnungen. Planner integriert sich dabei nahtlos in MS Teams und unterstützt die Projektplanung mithilfe visueller Diagramme.
- **Forms, Lists, To Do, Whiteboard**
  Eine Reihe von „kleineren“ Produktivitäts-Apps unterstützen das tägliche Arbeiten, indem diese einen Werkzeugkasten mit zusätzlichen Funktionen zur Verfügung stellen
- **Power BI**
  Die Basis Version Power BI unterstützt die Analyse und Visualisierung von Daten sowie die Erstellung von Berichten.

In Phase 2 wird geprüft, inwieweit diese Apps flächendeckend eingesetzt und dabei **Synergieeffekte und Lizenzeinsparungen** erzielt werden können. Nach erfolgreicher Prüfung einzelner Apps und datenschutz- sowie informationssicherheitsrechtlicher Freigabe erfolgt der Rollout der jeweiligen App.

5.2.3.5. Microsoft Defender

Ein weiterer Bestandteil des E3-Planes ist der **Virenschutz Microsoft Defender** in einer Basisversion, der eine grundlegende Funktionalität im Bereich der Absicherung des Windows Client Betriebssystems umfasst (Endpoint Security).

Hierbei wird überprüft, inwiefern diese Funktionen die **Anforderungen der IT-Security** erfüllen und das bisher von der Stadt Nürnberg eingesetzte Virenschutzprogramm Trellix ersetzen können.

5.2.3.6. E5-Plan-Funktionalitäten

Der M365 E3-Plan umfasst die beschriebenen Funktionalitäten aus den Teilen Office 365, Enterprise Mobility Suite 365 und Windows Client Betriebssystem.

Ein E5-Plan beinhaltet alle Funktionen des E3-Planes und ergänzt diese um die Funktionen:

- IT-Security,
- Governance und Compliance,
- Datenschutz und Kommunikation.

Es wird geprüft, inwiefern diese Funktionen zukünftig für die Stadt Nürnberg zum Einsatz kommen sollen und ob die Lizenzierung eines E5-Planes in der dritten Phase angestrebt wird.

E5 Security

Die E5 Security erweitert den Virenschutz Defender um spezifische Funktionen zum Schutz

- von Office 365 (z.B. Anti-Phishing, Absicherung von Attachments, sichere Links, verbesserte Bedrohungserkennung, etc.) und
- des Windows Betriebssystems um erweiterte Analysefunktionen und zentrale Management-funktionen.

In der Entra-ID werden Funktionen zum **Schutz der digitalen Identität** und zur **Steuerung des Zugriffes** hinzugefügt.

E5 Compliance

Ziel der E5 Compliance ist der Schutz interner Daten vor Abfluss oder unbefugter Weitergabe, das Risikomanagement und Auditfunktionalitäten.

E5 Produktivitäts-Apps

Die E5 Suite enthält einige zusätzliche oder funktional erweiterte Produktivitäts-Apps. Dies sind u.a. Power BI Pro mit der Funktion, Berichte zu verteilen, die Funktionalität Festnetz-Telefongespräche aus MS Teams zu führen und die volle Audiokonferenzfunktion von MS Teams mit bis zu 1.000 Teilnehmern.

5.3. Phase 3 – Kontinuierliche Weiterentwicklung des modernen Arbeitsplatzes

5.3.1. Zeitraum

Die Projektphase 3 beginnt nach Abschluss von Phase 2 - derzeitig geplant ab 2027.

5.3.2. Inhalte

- Ständiges Monitoring neuer Innovationen, Anpassung/Feintuning von Prozessen unter Nutzung neuer Möglichkeiten (z. B. KI).
- Bei Bedarf Einführung erweiterter Funktionalitäten aus dem E5-Plan in den Bereichen IT-Security, Governance & Compliance, Datenschutz und Telekommunikation

5.3.3. Beschreibung

Nach Einführung des modernen IT-Arbeitsplatzes auf Basis der M365-Suite soll eine kontinuierliche Weiterentwicklung der Arbeitsumgebung erfolgen. Microsoft veröffentlicht kontinuierlich neue Funktionen und Apps, deren möglicher Nutzen für die Stadt Nürnberg validiert werden müsste.

Fachliche Anforderungen der Sachgebiete können zukünftig mithilfe moderner M365 Funktionen wie beispielsweise Power Apps teilweise direkt im M365 Kontext umgesetzt werden. Hierfür bedarf es einer ständigen Weiterbildung und Schulung sowie einer agilen Vorgehensweise, um diese Potentiale für die Stadt Nürnberg zu heben und damit die Umsetzungsgeschwindigkeit massiv zu beschleunigen.

Im Bereich der Kommunikation kann MS Teams auf Basis einer E5-Lizenzierung perspektivisch zu einer Kommunikationsplattform ausgebaut werden, die neben den digitalen Kommunikationswegen (z.B.: E-Mail, Chat, Messaging, etc.) auch die klassische Festnetz-Telefonie integriert.

5.3.3.1. Erweiterte Security Funktionen eines E5-Lizenzpaketes

Durch die Nutzung von M365 werden Softwareaktualisierungen automatisch von Microsoft durchgeführt, so dass stets die **neuesten Funktionen und Sicherheitsupdates** ohne internen Aufwand zur Verfügung stehen.

Eine Migration – wie sie gerade bei Office 2016 ansteht - ist aus heutigen Gesichtspunkten in nächster Zeit nicht zu erwarten.

Hinsichtlich möglicher digitaler Bedrohungen und Cybergefahren ist bei Office 365 der Sicherheitsaspekt nicht zu vernachlässigen: Unternehmen jeder Größenordnung müssen sich weiterhin mit Sicherheitslösungen befassen, um Risiken wie schädliche Mail-Anhänge, Ransomware, Phishing oder Datendiebstahl zu entschärfen.

6. Zyklische Überprüfung der Strategie

Die **Verwendung von Microsoft 365 (M365)** bietet zahlreiche Vorteile, wie verbesserte Zusammenarbeit, effiziente Kommunikation und nahtlose Integration von Anwendungen. Dennoch ist es wichtig, sich der potenziellen Nachteile bewusst zu sein.

Vendor Lock-In ist ein Begriff, der auftritt, wenn ein Kunde eines bestimmten Produkts oder einer Dienstleistung daran gehindert wird, den Anbieter zu wechseln. Im Fall von M365 bedeutet dies, dass Unternehmen, die sich für M365 entscheiden, in das Microsoft-Ökosystem eingebunden werden. Dies kann zu Problemen führen, wenn sie später zu einem anderen Anbieter wechseln möchten. Die Gründe dafür sind vielfältig:

- **Proprietäre Technologien**: M365 nutzt proprietäre Technologien, die dem Betriebsgeheimnis unterliegen und nicht öffentlich zugänglich sind. Diese Technologien sind möglicherweise nicht kompatibel mit Lösungen anderer Anbieter.
- **Vertragliche Beschränkungen**: Verträge mit Microsoft können Klauseln enthalten, die den Wechsel zu einem anderen Anbieter erschweren. Dies kann zu Kosten führen und die Flexibilität des Unternehmens einschränken.
- **Abhängigkeit vom Hersteller**: Unternehmen, die M365 verwenden, sind von Microsoft abhängig. Ein Wechsel zu einem anderen Anbieter erfordert Zeit, Ressourcen und möglicherweise Anpassungen an bestehenden Prozessen.
- **Datenhoheit (Datensouveränität)**: Durch die Nutzung von M365 werden Daten in der Microsoft-Cloud gespeichert. Dies bedeutet, dass die Kontrolle über diese Daten teilweise an Microsoft übergeht. Die Stadtverwaltung wird sicherstellen, dass die Daten regelmäßig überprüft und sichergestellt wird, dass die volle Kontrolle darüber behalten wird.

Um einen **Vendor Lock-In** zu vermeiden, wird die Nutzung der diversen Funktionalitäten von M365 regelmäßig überprüft werden.

Derzeit ist ein Überprüfungszyklus von 24 Monaten geplant. Es wird geprüft, ob die Nutzung von M365 noch zu den aktuellen Anforderungen passt, ob Alternativen verfügbar sind und ob die strategische Positionierung der Produkte von Microsoft noch zu den Zielsetzungen der Stadtverwaltung passen.

Insgesamt ist M365 eine leistungsstarke Plattform, die Stadtverwaltung sollte sich aber der potenziellen Risiken bewusst sein und die Entscheidungen sorgfältig abwägen.