

Microsoft 365: Die digitale Transformation in der Verwaltung

EIN LEITFADEN FÜR ENTSCHEIDUNGSTRÄGER



Executive Summary	3
1. Microsoft 365 als Schlüssel zum produktiven Arbeiten	4
Anwendungsbeispiel 1: Kollaboratives Arbeiten im gleichen Dokument	5
Anwendungsbeispiel 2: Gleichzeitige Nutzung mehrerer Endgeräte.....	6
Anwendungsbeispiel 3: Sicheres und zielgerichtetes Teilen von Dokumenten	6
2. Behördliche Herausforderungen bei der Nutzung der Cloud	8
3. Microsoft 365 im Mehrmandantenbetrieb	10
4. Einführung von Microsoft 365	12
5. Fazit	14
6. Warum Arvato Systems	15
7. Kontakt	15

Executive Summary

Microsoft 365 ist der Schlüssel zur produktiven Büroarbeit unserer Zeit: Telefonie und Chats, Office-Anwendungen und Datei-Ablage, hohe IT-Sicherheit und effizienter Betrieb, einfach und integriert nutzbar. Zudem wird die Produktivitäts-Suite angereichert durch künstliche Intelligenz und ist stets sicher verfügbar in der aktuellen Version mit den neusten Funktionen. Lange war es Unternehmen, die sich im Besitz des Staates befinden, sowie Organen der öffentlichen Hand nicht möglich, auf cloudbasierte Lösungen zuzugreifen. Dank des EU-Angemessenheitsbeschlusses und der EU-Datengrenze von Microsoft können die meisten **öffentlichen Unternehmen heute Microsoft 365 nutzen, ohne rechtliche Hindernisse zu befürchten.** Für Behörden mit erweiterten Schutzbedarfen wird zukünftig die gemeinsam von SAP und Arvato Systems angekündigte DELOS-Cloud verfügbar sein, die auf Basis von Microsoft-Technologie eine souveräne und sichere Cloud-Plattform für die Digitalisierung des Öffentlichen Diensts in Deutschland darstellt.

Viele öffentliche Organisationen lassen die IT ihrer Arbeitsplätze von eigenen IT-Dienstleistern betreuen. Diese bedienen dann neben kommunalen oder regionalen Behörden auch privatwirtschaftlich geführte Unternehmen wie Stadtwerke und Nahverkehrsbetriebe, aber auch Schulen. Eine **Kundenstruktur mit sehr unterschiedlichen Schutzbedarfen** und inhaltlichen Anforderungen. Die Leistungserbringung dieser IT-Dienstleister ist ebenfalls heterogen: Um einen den heutigen Anforderungen entsprechenden IT-Arbeitsplatz im eigenen Rechenzentrum bereitstellen zu können, müssen mehrere spezialisierte Teams viele Anwendungen diverser Hersteller betreiben und integrieren. **Die Gewährleistung der IT-Sicherheit** ist eine besondere Herausforderung, da die zahlreichen hersteller- und kundenspezifischen Integrationen die erforderlichen, regelmäßigen Updates erschweren.

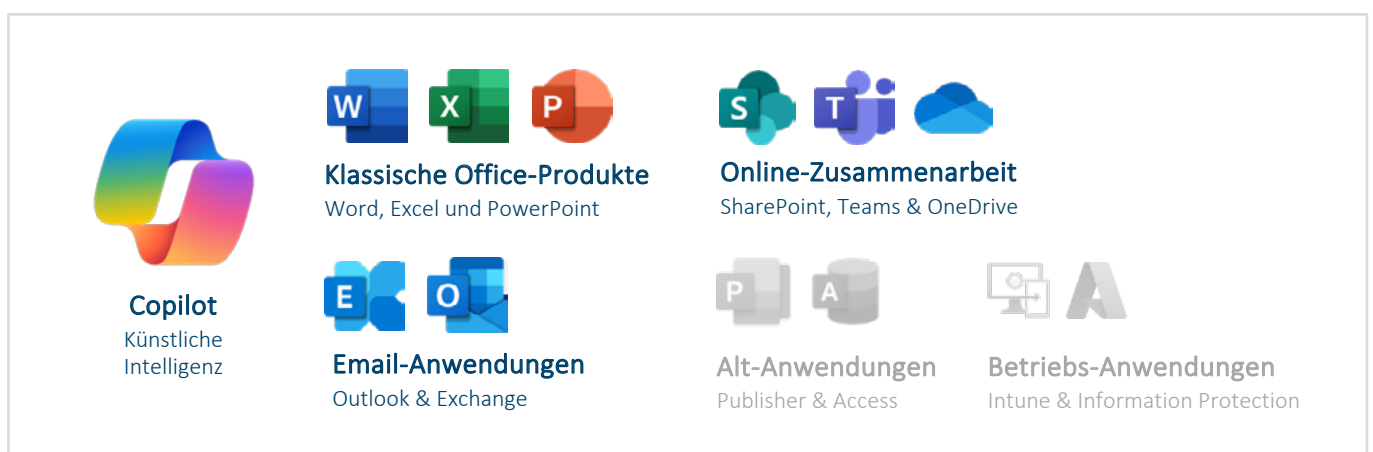
Microsoft und Arvato Systems bieten den IT-Dienstleistern hierfür eine attraktive Gesamtlösung. **Mit dem Microsoft Cross-Tenant Access** können **unterschiedliche Schutzbedarfe skalierbar und effizient** durch ein zentrales Team des Dienstleisters erfüllt werden. Durch NAVOO® von Arvato Systems wird zudem eine Governance-Ebene eingeführt, welche die **Kunden-Organisationen vor Fehlkonfigurationen** schützt und bei der Einführung von Best Practices unterstützt.

Insgesamt bringt die Umstellung auf eine Cloud-Lösung viele Vorteile für die Nutzer:Innen: Gleichzeitig am gemeinsamen Dokument arbeiten, zwischen verschiedenen Endgeräten wechseln, einfach und sicher Links zu Inhalten verschicken – all dies schafft **Komfort und Produktivität am Arbeitsplatz.** Noch wichtiger aber sind die Vorteile im Bereich Cybersecurity: Mit Microsoft 365 als Cloud-Lösung sind alle Anwendungen, Komponenten und Services, die mit der Arbeitsplatz-IT verbunden sind, stets auf dem **aktuellsten Stand der Sicherheit.** All diese Punkte sprechen dafür, dass Organisationen, die noch klassische Arbeitsplatz-IT nutzen, sich **baldmöglichst** mit dem Potential von Microsoft 365 beschäftigen und einen Umstieg in Erwägung ziehen sollten

1. Microsoft 365 als Schlüssel zum produktiven Arbeiten

Der moderne Arbeitsplatz mit Microsoft 365 – umfassende Funktionen und Benutzerfreundlichkeit

Der Arbeitsplatz im Büro hat sich deutlich gewandelt – in der Verwaltung, der Industrie und auch im privaten Bereich. Anstelle der klassischen Arbeitsmittel (Telefon, Brief, Kalender, Archiv etc.) verwenden wir heute Software-Funktionen, die uns das Leben erleichtern. Die Software-Funktionen wurden zunächst auf dem stationären Computer genutzt und später durch eine Reihe von mobilen Endgeräten (Mobiltelefon, Laptop, iPad etc.) ergänzt, die für die gleichen Funktionen und Inhalte optimierte Bedienoberflächen bieten.



Grafik 1: Die bekanntesten der über aktuell 190 Services von M365.

Mit Microsoft 365 stellt Microsoft eine umfassende innovative Software Suite zur Verfügung, die alle Funktionen des modernen Arbeitsplatzes enthält: Office-Anwendungen wie Word, Excel und PowerPoint, (Video-) Telefonie, E-Mails und Datei-Ablage. Auch die Zusammenarbeit in dedizierten Teams sowie die unternehmensinterne Kommunikation wird erleichtert. Selbst Alt-Anwendungen, so genannte Legacy Software, wie **Microsoft Publisher** (für Grafikdesign) und **Microsoft Access** (zur Erstellung eigener Datenbanken) stehen weiterhin zur Verfügung.

Die Suite umfasst auch Services wie **Microsoft Intune** (Verwaltung von physischen und virtuellen Endgeräten) sowie **Microsoft Purview Information Protection** (Organisation und Schutz sensibler Daten).

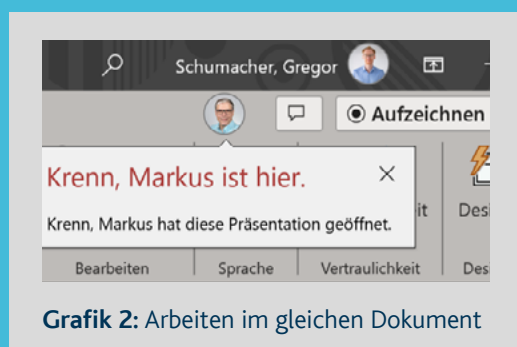
Besonders hilfreich in der alltäglichen Arbeit ist die von Microsoft entwickelte Funktion **Copilot**. Mit diesem Service steht den Anwender:innen ein virtueller Assistent zur Seite. Er kann unter anderem Dokumente zusammenfassen, Texte und Präsentationen erstellen sowie Tabellen übertragen und vervollständigen. **Microsoft 365 Copilot** verwendet dabei nur die Daten, die für die Nutzer:innen freigegeben sind.

Nahtlose Integration aller Services – zuhause oder im Büro auf allen Endgeräten

Ein wesentlicher Vorteil von Microsoft 365, im Vergleich zu anderen Produktivitätslösungen am Markt ist die hohe Integrationstiefe aller Services. Die Funktionen sind untereinander nahtlos integriert und können sowohl vom klassischen Desktop-PC als auch über mobile Endgeräte genutzt werden. Mitarbeitende können vom Büro, aus dem Home Office oder dem Internet-Café arbeiten und über verschiedene Tools auf die gleichen Inhalte zugreifen. Für alle Anwendungen gilt das gleiche Passwort (Single Sign-On). Dank der Multi-Faktor-Authentifizierung (MFA) und **Windows Hello for Business** auf den Endgeräten, ist die Nutzung von M365 somit benutzerfreundlich und sicher. Im Folgenden werden einige Beispiele dargestellt, wie Microsoft 365 die Produktivität am Büro-Arbeitsplatz durch Benutzerfreundlichkeit und Service-Integration erhöht.

ANWENDUNGSBEISPIEL 1 Kollaboratives Arbeiten im gleichen Dokument

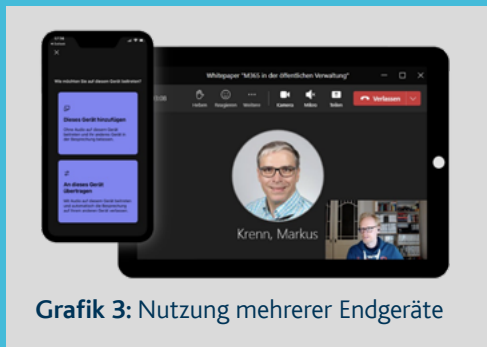
Ein gutes Dokument ist das Ergebnis einer gelungenen Teamarbeit. Ein:e Kolleg:in legt die Struktur fest und verfasst einen ersten Entwurf. Dann bringen verschiedene Expert:innen ihr Know-how in die einzelnen Kapitel ein. Andere Team-Mitglieder schreiben eine einladende Einleitung, gestalten ansprechende Bilder und sorgen für eine fehlerfreie Sprache. Früher mussten Projektleitende die Bearbeitungsreihenfolge aufwändig choreographieren. Nun können alle Mitarbeitenden gleich-



zeitig im Dokument arbeiten. Wer gerade welche Passage im Dokument bearbeitet, wird in der Benutzeroberfläche angezeigt (siehe Grafik 2). Änderungen aller Team-Mitglieder sind live über alle Endgeräte hinweg verfügbar. Die Versionierung der Dateien erfolgt automatisch im Hintergrund. Wenn also etwas schiefgeht, kann das Team auf vorherige Versionen des Dokuments zugreifen.

ANWENDUNGSBEISPIEL 2 Gleichzeitige Nutzung mehrerer Endgeräte

Die Arbeit ist nicht mehr an einen festen Ort oder Rechner gebunden. Mitarbeitende wollen sich flexibel und mobil vernetzen, egal ob sie vom Büro zum Meetingraum, vom Schreibtisch zur Kaffeemaschine oder vom Auto nach Hause gehen.

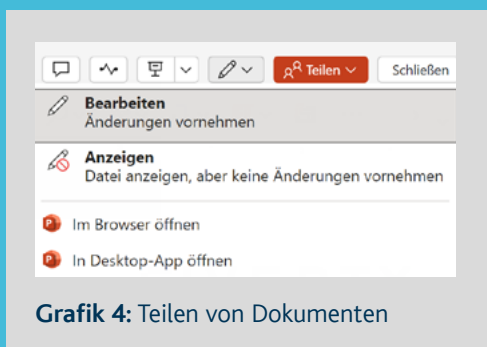


Grafik 3: Nutzung mehrerer Endgeräte

Mit Microsoft 365 können sie ihre Endgeräte problemlos und sicher miteinander verbinden. Nutzer:innen können mehrere Geräte gleichzeitig nutzen, um zum Beispiel ihren Bildschirm vom PC zu teilen, aber Ton und Kamera vom Handy zu verwenden. Auch die unterbrechungsfreie Übergabe von Gesprächen zwischen Geräten ist möglich.

ANWENDUNGSBEISPIEL 3 Sicheres und zielgerichtetes Teilen von Dokumenten

Für die Suche und Weiterleitung von Informationen geht oftmals viel Zeit verloren, da eine Vielzahl von Dateien und Ablagen den Prozess erschwert. Zudem ist nicht immer klar: Sind meine Inhalte nach erfolgter Weiterleitung immer noch sicher? Mit Microsoft 365 hingegen versenden

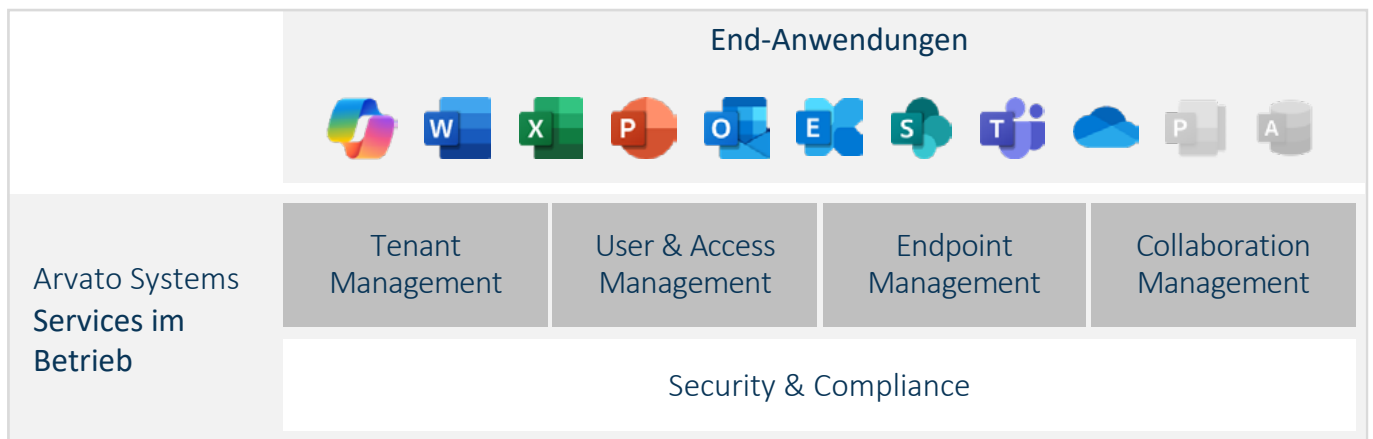


Grafik 4: Teilen von Dokumenten

Verfasser:innen nicht das Dokument, sondern einen individuellen Link auf das ausgewählte Dokument. Bei der Erstellung des Verweises können die Nutzer:innen definieren, welche Kolleg:innen (einzelne Personen oder Gruppen) auf den Inhalt zugreifen dürfen. Dabei kann auch bestimmt werden, wie lange und mit welchen Rechten (Schreib- oder Leserechte) die Bearbeitung vorgenommen werden kann.

Umfangreiche Betriebsleistungen und sichere Anwendungen

Die Welt der Arbeitsplatz-IT hat eine verborgene Herausforderung: Der sichere Betrieb der Anwendungen. Im Falle der Migration zu M365 werden Infrastruktur-nahe und Kern-Software-bezogene Tätigkeiten durch Microsoft übernommen. Darüber hinaus verbleiben einige Betriebs-Themen wie Konfiguration, Nutzer:innen-Administration und Endgeräte-Management weiterhin beim Kunden.



Grafik 5: Betriebsaufgaben rund um M365

Wichtige Tätigkeiten zur Absicherung der Workplace-Suite:

- ✓ **Tenant Management:** Alle Nutzer:innen von Microsoft 365 sind einem Mandanten zugeordnet. Dort erfolgt die zentrale Verwaltung und Konfiguration der jeweiligen Organisation.
- ✓ **User & Access Management:** Automatisiertes und sicheres On- und Offboarding von neuen Kolleg:innen mit den jeweiligen Rechten für ihre Rolle, Gruppe, Abteilung und Bereich.
- ✓ **Endpoint Management:** Im Zuge dieses Services wird die Software der Endgeräte aktualisiert und die Geräte-Compliance insgesamt her- und sichergestellt (z.B. Festplatten-Verschlüsselung, lokale Firewall).
- ✓ **Collaboration Management:** An dieser Stelle erfolgt die Administration der Einstellungen für die Tool-übergreifenden Zusammenarbeitsfunktionen der Organisation.
- ✓ **Device Lifecycle Management:** Inbetriebnahme und Updates der Endgeräte auch im Home Office ohne Vor-Ort-Präsenz im eigenen Netzwerk.

Besonders relevant sind die umfassenden Sicherheits- und Compliance-Services, mit denen die wichtigsten Einfallstore für Viren und andere Bedrohungen der IT-Sicherheit erkannt und abgesichert werden (Vulnerability Management). Zudem werden die Zugangsinformationen der Nutzer:innen geschützt, Sicherheitsvorfälle erkannt und Maßnahmen zu deren Bekämpfung eingeleitet (Endpoint Detection & Response).



2. Behördliche Herausforderungen bei der Nutzung der Cloud

Organisationen des öffentlichen Dienstes haben unterschiedliche Schutzbedarfe

Kollaboratives Arbeiten im selben Dokument, flexible Nutzung mehrerer Endgeräte, einfacher Zugriff per Link und ständige Innovationen: Diese Funktionen von Microsoft 365 wurden erst durch die Entwicklung der Cloud-Technologie möglich. Warum nutzen bis heute nur so wenige staatliche Organisationen diese Vorteile? Der Grund liegt in den hohen Schutzbedarfen der öffentlichen Hand. Während sich privatwirtschaftliche Unternehmen darauf konzentrieren, den Datenschutz einzuhalten und die Sicherheit von Rechenzentren und Software zu gewährleisten, müssen Behörden sich auf den Eintritt besonderer Risiken vorbereiten.

Zu solchen Risiken gehören insbesondere geopolitische Konflikte mit außereuropäischen Akteuren, welchen mit einer besonderen Absicherung des Betriebs der Cloud sowie der Hard- und Software-Wertschöpfungsketten begegnet wird.

	Privatwirtschaftliche Unternehmen in öffentlicher Hand	Offizielle Organe der öffentlichen Hand
	Bsp: Transport-Unternehmen, Stadtwerke, ...	Bsp: Behörden von Bund, Land und Kommunen
Grundlegende Schutzbedarfe	• Strikte Einhaltung des Datenschutzes (insb. DSGVO) • Allgemeine physikalische Sicherheit der Rechenzentren (z.B. gemäß C5) • Absicherung gegen Cyberkriminalität	
Erweiterte Schutzbedarfe	In der Regel nicht vorhanden	• Absicherung der Software-Wertschöpfungskette • Absicherung der Hardware-Wertschöpfungskette • Absicherung gegenüber geopolitischen Krisen

Grafik 6: Unterschiedliche Schutzanforderungen

Microsoft bietet für alle Schutzbedarfe die passende Cloud

Der Wandel von der klassischen IT zu integrierten Cloud-Lösungen ging vor allem von US-Unternehmen aus. Mit dem Aufbau der ersten Cloud-Rechenzentren in Europa im Jahr 2009 konnten Unternehmen auch ihre Inhaltsdaten lokal speichern. Um ihre Services zuverlässig zu betreiben und weiterzuentwickeln, musste Microsoft bis vor kurzem noch einige Telemetrie- und Supportdaten aus Europa auslagern.

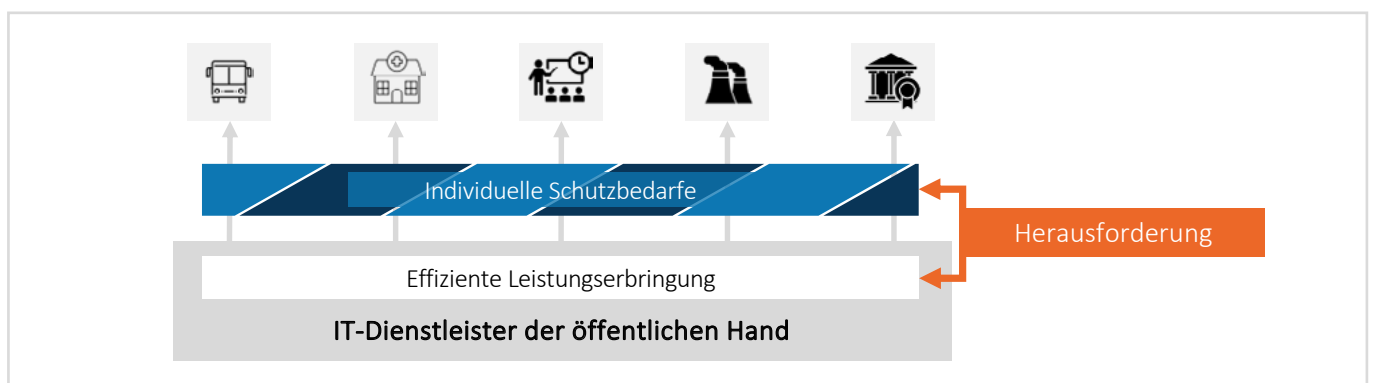
	Grundlegende Schutzbedarfe		Erweiterte Schutzbedarfe
Cloud-Angebot	 Microsoft Cloud	 Microsoft Cloud mit Datengrenze	 DELOS mit Microsoft Technologie
Inhaltsdaten			
Telemetrie & Supportdaten			
Betrieb	durch ein europäisches Tochter-Unternehmen von Microsoft		durch SAP / Arvato Systems
Datenschutz	durch Angemessenheitsbeschluss der EU oder durch Datenschutzfolgeabschätzung		technisch kein ungewünschter Datentransfer möglich

Grafik 7: Clouds für unterschiedliche Schutzbedarfe

Microsoft hat 2023 eine „EU-Datengrenze“ schrittweise umgesetzt. Diese Option ermöglicht es Kunden, zu entscheiden, ob sie neben ihrer Inhalts- auch ihre Telemetrie- und Support-Daten in der EU behalten wollen. Für einen noch höheren Schutzbedarf bietet Microsoft ab voraussichtlich 2026 die DELOS-Cloud an.

Kunden von IT-Dienstleistern der öffentlichen Hand haben unterschiedliche Schutzbedarfe

Viele der heutigen Lösungen für Arbeitsplatzumgebungen werden von lokalen, öffentlichen IT-Dienstleistern angeboten. Sie betreuen neben Behörden mit erweiterten Schutzbedarfen häufig auch privatwirtschaftlich organisierte Unternehmen, die sich im öffentlichen Besitz befinden. Diese übernehmen weniger hoheitliche Aufgaben und ähneln in ihren Anforderungen eher Privatunternehmen. Diese heterogene Lage erschwert es den Dienstleistern, ihren Kunden ein einheitliches und skalierendes Angebot von hoher Qualität zu liefern.

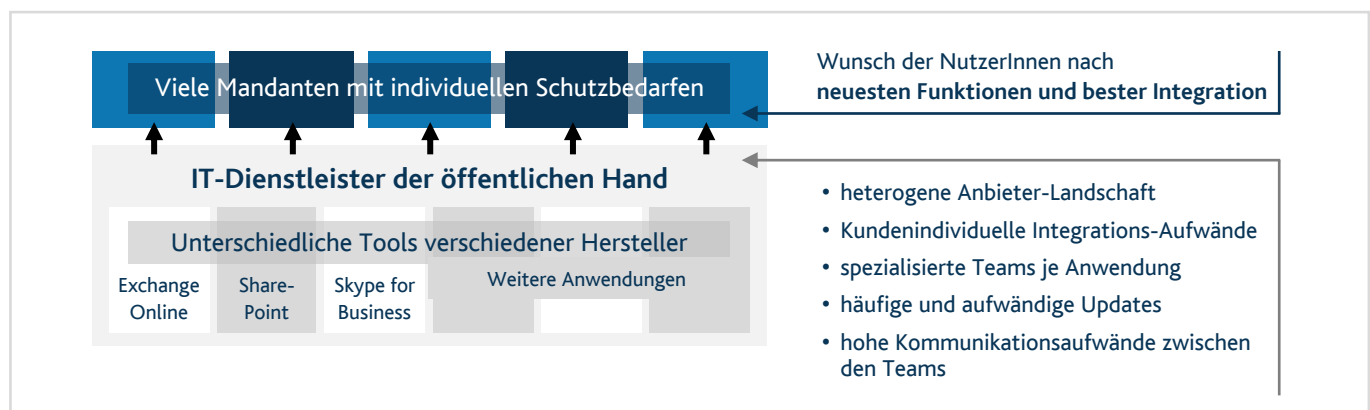


Grafik 8: Effiziente Leistungserbringung vs. heterogene Kundenstruktur

3. Microsoft 365 im Mehrmandantenbetrieb

Der sichere Betrieb der heterogenen Arbeitsplatz-IT ist sehr herausfordernd

In vielen Fällen wird die Komplexität des IT-Betriebs durch interne Herausforderungen weiter erhöht. Die meisten Arbeitsplatz-Lösungen bestehen aus Softwares unterschiedlicher Anbieter. Für Betrieb und Sicherstellung regelmäßiger Updates benötigt der IT-Dienstleister jeweils spezialisierte Teams je Tool.



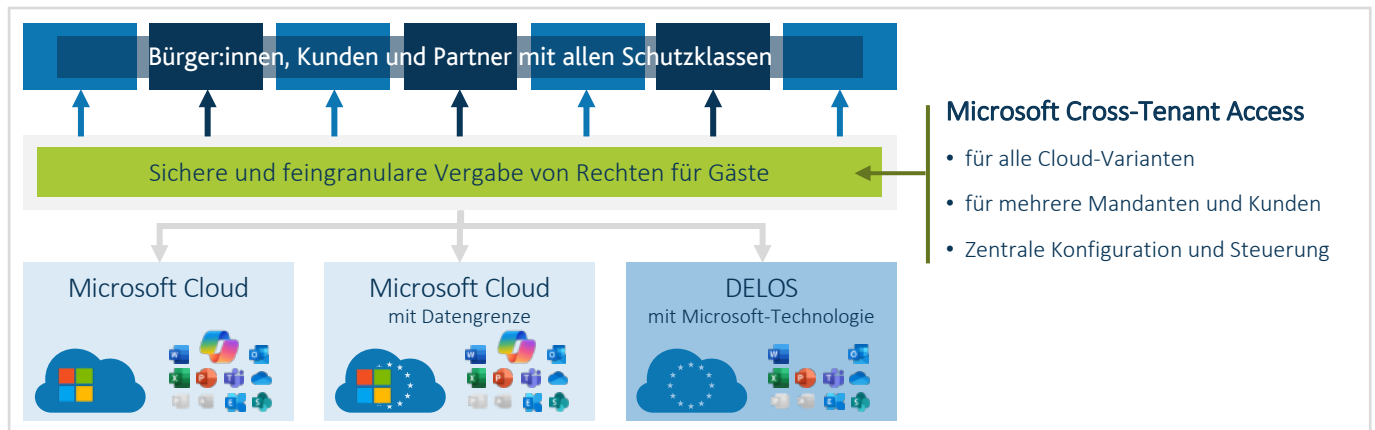
Grafik 9: Interne Herausforderungen im IT-Betrieb klassischer Arbeitsplatz-IT

Um dem Wunsch der Nutzer:innen nach nahtloser Nutzung der auf viele Anwendungen verteilten Funktionen nachzukommen, entstehen hohe Integrations-Aufwände. Hierfür muss der IT-Dienstleister die Kundenwünsche aufnehmen, Änderungsaufträge spezifizieren, die betroffenen Teams identifizieren, übergreifende Umsetzungsprojekte steuern und Change-Management betreiben.

Sind diese kundenspezifischen Anpassungen umgesetzt, führen sie zwar kurzfristig zu einer höheren Zufriedenheit bei den Nutzer:innen, mittel- und langfristig aber erschweren sie die Durchführung von Standard-Updates für die jeweiligen Einzel-Anwendungen. Updates werden aufwändiger und somit seltener durchgeführt. Dies kann wiederum zu Sicherheitsmängeln führen.

Sichere Zusammenarbeit auch über unterschiedliche Schutzklassen hinweg

Microsoft hat die Anforderungen seiner Partner identifiziert und eine Lösung speziell für Organisationen erarbeitet, die trotz hoher eigener Schutzklasse mit externen Kunden und Partnern sicher und flexibel zusammenarbeiten wollen: Microsoft Cross-Tenant Access.



Grafik 10: MS-Cross-Tenant Access zur sicheren und flexiblen Zusammenarbeit mit Kunden und Partnern

Mit Hilfe dieser Funktion können auch sehr diverse Dokumente mit Bürger:innen, Kunden und Partnern in einem besonders abgeschotteten Raum sicher austauschen. Die Freigabe von Rechten erfolgt dabei sehr feingranular, beispielsweise differenziert nach Individuen oder Nutzergruppen, zeitlich begrenzt und nur mit Lese- oder auch Schreibrechten. Voraussetzung hierfür ist die Nutzung der weit verbreiteten [Microsoft Entra-ID](#) (vormals [Azure Active Directory](#)).

Arvato Systems NAVOO® stellt zusätzliche Governance sicher

Microsoft 365 reduziert die Mühen für Anwender-Organisationen deutlich: Weniger Aufwände für Betrieb, Integration, Projekte, Updates und IT-Sicherheit. Die Verantwortung, die zahlreichen Optionen und Einstellungsmöglichkeiten der Arbeitsplatz-Suite zielgerichtet und sicher zu konfigurieren, verbleibt dennoch beim Kunden oder dessen IT-Dienstleister. Um diese Aufgabe zu vereinfachen, hat Arvato Systems NAVOO® entwickelt. Dieser Software as a Service (SaaS) unterstützt Anwender dabei, Microsoft 365 effizient einzuführen, aktuell zu halten und zu überwachen. Zudem hält NAVOO® umfangreiche Vorlagen und Prozesse etwa für Namenskonventionen, Berechtigungen und Rollenkonzepte vor.



Grafik 11: Arvato Systems NAVOO® für unkomplizierte Governance

4. Einführung von Microsoft 365

Vom klassischen Rechenzentrum in die Cloud

Ist die Entscheidung für eine Modernisierung der Arbeitsplatz-IT gefallen, geht es darum, die Migration erfolgreich zu gestalten. Auf dem Weg von der heterogenen IT-Landschaft eines klassischen Rechenzentrums mit vielen spezialisierten Teams hin zum skalierenden Betrieb einer Cloud-Lösung gibt es einige Herausforderungen.



Grafik 12: Herausforderungen beim Übergang zu M365.

Neben der Durchführung der technischen Migration muss vor allem das Identitäts-Management der beteiligten Organisationen neu gedacht werden. Dieses basiert in der Regel noch auf lokalen Active Directory-Konzepten und muss mit der Nutzung von Microsoft Entra-ID (vormals Azure Active Directory) an die Paradigmen der Cloud angepasst werden, um die hiermit verbundenen Chancen auch wirklich zu nutzen.

Mit der Öffnung des IT-Arbeitsplatzes für unterschiedliche Endgeräte außerhalb des eigenen Netzwerkes entstehen neue Sicherheits-Herausforderungen. Im Rahmen der Einführung von M365 wird diesen durch die Einführung des neuen Sicherheits-Paradigmas „Zero Trust“ begegnet. User werden nicht mehr automatisch als vertrauenswürdig angenommen, sobald sie sich im Netzwerk der Orga-

nisation befinden: sie müssen sich ständig authentifizieren und erhalten nur die minimal notwendigen Rechte. Zudem werden die Netzwerke in deutlich kleinere Segmente unterteilt.

Arvato Systems nutzt für die Ablösung von lokalen Arbeitsplatz-Anwendungen durch Microsoft 365 ein erprobtes, vierstufiges Verfahren. In der ersten Stufe wird die Ist-Situation mit ihren jeweiligen Tools und Abhängigkeiten analysiert, sowie gemeinsam mit der Anwender-Organisation der Zielzustand definiert. Mit dem offiziellen Startschuss des Projektes wird die Projektorganisation aufgebaut und früh mit einer Pilotierung begonnen. Die dort gewonnene Praxiserfahrung steigert die Verlässlichkeit der Feinkonzepte.



Grafik 13: Einführung von Microsoft 365 in vier Stufen

Die Einführung von Microsoft 365 erfolgt stufenweise für verschiedene Anwendergruppen und wird begleitet durch umfangreiche, interne Kommunikation sowie Schulungs- und Coaching-Angebote. Letztere sind ein wichtiger Schlüssel für den dauerhaften Erfolg des neuen IT-Arbeitsplatzes, denn mit Microsoft 365 verbessert sich nicht nur der Funktionsumfang der Software der End-Anwender:innen, sondern auch der Aufgabenbereich der IT-Abteilung. Frühzeitige Information und Einbeziehung in Kombination mit aktivem Feedback-Einholen von den Nutzer:innen und den Admins steigert die langfristige Zufriedenheit mit der Lösung deutlich. Mit dem Abschluss des Projektes wird Microsoft 365 in einen dauerhaften Betrieb überführt.

Schon heute beginnen und Erfahrungen für Mandanten mit erweitertem Schutzbedarf nutzen

IT-Dienstleister von öffentlichen Organisationen sollten schon heute beginnen, ihre Kunden mit normalem Schutzbedarf nach Microsoft 365 zu überführen. Zum einen wird durch die Leistungsvielfalt der Office-Suite die Produktivität der betroffenen Mitarbeitenden deutlich erhöht. Zum anderen bietet Microsoft 365 für die meisten Organisationen mit normalem Schutzbedarf deutliche Fortschritte im Bereich der IT-Sicherheit. Die Cloud-Rechenzentren von Microsoft sind nach ISO27001 und C5 zertifiziert und die Milliarden-Investitionen des Cloud-Anbieters in Security-Operations-Center (SOC) sorgen für ein hohes Maß an Cybersicherheit. Sollten Sicherheitslücken auftreten, werden diese früh erkannt und dank der vierstelligen Zahl monatlicher Updates schnell behoben.

Für IT-Dienstleister bietet der zeitige Beginn der Migration ihrer Kunden weitere Vorteile: Durch ein schrittweises Vorgehen werden die eigenen, knappen Ressourcen nicht überlastet. Lerneffekte entstehen früh und können für nachfolgende Projekte genutzt werden. Auch können die durch den neuen Leistungsschnitt entstehenden internen Veränderungen besser gesteuert werden.



5. Fazit

Die Cloud hat die Arbeitsplatz-IT revolutioniert. Microsoft 365 bietet Anwender:innen mehr Funktionalität und Nutzerfreundlichkeit, was zu einer Steigerung der Produktivität führt. Die Cloud-Lösung erleichtert auch den IT-Betrieb: Bessere IT-Sicherheit dank kontinuierlicher und automatischer Updates und höhere Informations-Sicherheit durch stets aktuelle Governance-Best-Practices.

Microsoft hat seine Produktivitäts-Suite an verschiedene Schutzbedarfe angepasst. Kunden, die Datenschutz, physikalische Sicherheit und Cybersecurity wichtig finden, können das klassische Microsoft 365 oder ein Microsoft 365 mit EU-Datengrenze wählen. Organisationen mit speziellen Schutzbedarfen wie beispielsweise Behörden können für besonders schutzwürdige Bereiche zukünftig die DELOS-Cloud nutzen. Diese von den deutschen Partnern SAP und Arvato Systems angekündigte „Souveräne Cloud“ basiert auf Microsoft-Technologie und wird in deutschen Rechenzentren unabhängig betrieben. Die wesentlichen Voraussetzungen für den Weg in die Cloud sind also bereits vorhanden, die abschließenden Schritte für spezielle Schutzbedürfnisse sind zudem angestoßen.

Um sich zukunftssicher aufzustellen, sollten öffentliche Unternehmen, Behörden und die jeweiligen IT-Dienstleister daher schnell mit ersten Cloud-Migrationen ihrer Produktivitäts-Lösungen beginnen. Damit erfüllen sie nicht nur die Erwartungen ihrer Anwender:innen an eine moderne und integrierte Arbeitsplatz-IT, sondern senken auch ihre Betriebskosten und verbessern oft ihre IT-Sicherheit.



6. Warum Arvato Systems

Arvato Systems unterstützt als international agierender IT-Spezialist namhafte Unternehmen bei der Digitalen Transformation. Ausgeprägtes Branchen-Know-how, hohes technisches Verständnis und ein klarer Fokus auf Kundenbedürfnisse zeichnen uns aus. Im Team entwickeln wir innovative IT-Lösungen, bringen unsere Kunden in die Cloud, integrieren digitale Prozesse und übernehmen den Betrieb sowie die Betreuung von IT-Systemen.

Als Teil von Bertelsmann stehen wir auf dem soliden Fundament eines deutschen Weltkonzerns. Zugleich setzen wir auf unser starkes strategisches Partner-Netzwerk mit internationalen Top-Playern wie AWS, Google, Microsoft oder SAP. Wir machen die digitale Welt einfacher, effizienter und sicherer und unsere Kunden erfolgreicher.

We Empower Digital Leaders.

arvato-systems.de

Weitere Fragen?

Nehmen Sie Kontakt mit uns auf:

Arvato Systems GmbH
Markus Krenn
Bereichsleiter Digital Workplace Arvato Systems
Reinhard-Mohn-Straße 18
33333 Gütersloh
Tel.: +49 (89) 4136 8155
microsoft-solutions@bertelsmann.de
arvato-systems.de