Arvato Systems Whitepaper

Effizienzblocker in der digitalen Arbeitsumgebung

Smarte Lösungsansätze für gezielte Effizienzsteigerung im Digital Workplace

ARVATO SYSTEMS

START

DARUM GEHT ES IN DIESEM WHITEPAPER

Die zunehmend dezentrale Energieerzeugung und Digitalisierung stellt Unternehmen aus dem Energiesektor vor große Herausforderungen. Eine Cloud hilft dabei, mit effizienten und schnellen Prozessen wettbewerbsfähig zu bleiben. Lokale IT-Infrastrukturen durch moderne Cloud-Systeme abzulösen, ist deshalb längst kein Trend mehr, sondern vermehrt Praxis in vielen Unternehmen.

Das zeigt vor allem die zunehmende Beliebtheit von Microsoft 365 für den „digitalen Arbeitsplatz“. So verwenden beispielsweise täglich über 145 Millionen Nutzende Microsoft Teams – dieser Wert hat sich innerhalb eines Jahres verdoppelt. Immer mehr Betriebe profitieren von den vielen Vorteilen, die ihnen Microsoft 365 bietet. So können sie in kurzer Zeit auch im Home-Office komplette digitale Arbeitsplätze bereitstellen. Das erleichtert die Zusammenarbeit, erhöht die Zufriedenheit der Mitarbeitenden und stärkt den Zusammenhalt im Unternehmen.

Eine schlechte oder unzureichende Einführung von Microsoft 365 führt hingegen zu erheblichen Effizienzverlusten und Sicherheitsproblemen. Der tägliche Unternehmensbetrieb erlaubt es meist nicht, Aspekte wie die Konzeption, Planung und Schulungen zu priorisieren – vor allem in Krisenzeiten wie der Corona-Pandemie.

In unserem Whitepaper stellen wir Ihnen Lösungsansätze sowie das Konzept und Angebot der Managed Services vor. Mit der Hilfe eines externen Dienstleisters können Sie das Management von Microsoft 365 professionalisieren. Darüber hinaus gehen wir auf mögliche Konflikte in den Bereichen Sicherheit, Governance, Compliance, Infrastruktur, Adoption und Geschäftsprozesse ein und zeigen, wie sich die Problemstellen auf die Produktivität der Mitarbeitenden und den Unternehmenserfolg auswirken.

Erfahren Sie, wie Sie einen modernen Arbeitsplatz nachhaltig im Unternehmen etablieren und was Sie dafür brauchen. Dabei kommt es vor allem auf zwei wesentliche Faktoren an:

- Für den Umstieg auf Microsoft 365 sollten Sie ein ganzheitliches Planungs-, Design- und Servicekonzept entwickeln.
- Es braucht Zeit bis die Prozesse technisch und organisatorisch umgesetzt sind, die Mitarbeitenden sie adaptieren und eine offene Unternehmenskultur annehmen.

Mit einem durchdachten Managementkonzept können Sie das große Potenzial des digitalen Arbeitsplatzes voll ausschöpfen.

GENERELLE ANFORDERUNGEN AN DEN DIGITALEN ARBEITSPLATZ

Der digitale Arbeitsplatz mit Microsoft 365 ist ein sehr komplexes System. Microsoft 365 allein besteht aus über dreißig Apps und Anwendungen (OneDrive, SharePoint, Exchange, Teams usw.) mit Hunderten von Features, die einzeln oder in Kombination miteinander funktionieren.

Ein Blick in die Admincenter der einzelnen Applikationen zeigt die Fülle von Konfigurationsmöglichkeiten – alle mit möglichen Auswirkungen auf die Sicherheit, Funktionsfähigkeit und Anwendungserfahrung der Mitarbeitenden.
Deshalb ist ein umfassendes Konzept, das die technischen und organisatorischen Voraussetzungen der Einführung und des laufenden Betriebes festlegt, essenziell für eine erfolgreiche, sichere und effiziente Nutzung von Microsoft 365.

Das Konzept muss dabei einen Ausgleich schaffen zwischen den Interessen der Mitarbeitenden und den Interessen des Unternehmens. Konkret bedeutet dies:

- Die Mitarbeitenden brauchen und erwarten eine überall funktionierende und einfach zu bedienende digitale Arbeitsumgebung, mit der sie ihre Aufgaben und Arbeiten schnell und effizient erledigen können. Egal ob im Büro, im Home-Office oder unterwegs: Die Kommunikation und Zusammenarbeit intern und extern soll überall funktionieren. Die Anforderungen der Mitarbeitenden tendieren hier zu einer Umgebung mit wenigen Beschränkungen und hoher Flexibilität.
- Das Unternehmen braucht Sicherheit, denn offene Systeme und heterogene Infrastrukturen bergen hohe Risiken. Sei es durch mutwilligen oder unbeabsichtigten Datenverlust, böswillige Cyber-Attacken oder der Verletzung von gesetzlichen Bestimmungen zum Datenschutz. Deshalb tendieren Unternehmen zu einer eher kontrollierten und restriktiven Umgebung.

Es ist ein Balanceakt zwischen dem Produktivitätsanspruch der Mitarbeitenden und dem Sicherheitsbedürfnis des Unternehmens – so viel Freiheit wie möglich, um flexibel und effektiv arbeiten zu können und so restriktiv wie nötig, um Sicherheitsrisiken zu minimieren.

Microsoft 365 bietet ein umfangreiches Funktionsset, um diesen Ausgleich in die Praxis umzusetzen. Dafür, und das können wir an dieser Stelle nur nachdrücklich betonen, ist ein umfassendes Konzept für Planung, Management des laufenden Betriebs und Training der Mitarbeitenden erforderlich.

Darüber hinaus stehen Unternehmen vor der Entscheidung, die Kompetenz, das Wissen und die Manpower für das Management von Microsoft Inhouse einzusetzen oder auf spezialisierte, externe Dienstleister zu setzen – für das gesamte Management oder nur Teile davon.

EFFIZIENZBLOCKER IN MICROSOFT 365

Schauen wir uns zunächst anhand einiger Beispiele an, welche Auswirkungen schlechte Deployments auf die Effizienz verschiedener Bereiche des digitalen Arbeitsplatzes haben können.

Effizienzblocker in der Sicherheit

Wie kann ich meine Unternehmensdaten und Infrastruktur vor unberechtigtem Zugriff, Hacker-Angriffen, Ransomware-Attacken und Datenverlust schützen? Sicherheitsmängel können schwerwiegende Folgen haben – Microsoft Studien gehen davon aus, dass die globalen durchschnittlichen Kosten für ein Datenleck bei rund vier Millionen US-Dollar liegen.

Eine Ransomware-Attacke, die den gesamten Datenbestand des Unternehmens verschlüsselt, ist nicht nur ein Effizienzblocker, sondern gefährdet, oder im schlimmsten Fall vernichtet, die Existenz des Unternehmens. Wie wichtig Schutzmaßnahmen für das Unternehmen sind, zeigen die Beispiele der häufigsten Risikoszenarien im Jahr 2021 im Microsoft Digital Defense Report:

- E-Mail-Phishing ist eine Hauptangriffsfläche: 70 Prozent aller Datenschutzverletzungen entstehen durch kompromittierte E-Mails. Microsoft blockiert im Jahr über 32 Milliarden schädlicher E-Mails mit steigender Tendenz.
- Malware wird immer öfter als legitimes Software-Update getarnt. Mitarbeitende installieren die Malware in Unkenntnis und ermöglichen so Angriffe.
- Ransomware-Attacken auf Unternehmen nehmen zu, mit denen die Angreifer die Datenbestände der betroffenen Unternehmen verschlüsseln und Lösegeld erpressen.

Lösungsansatz für effiziente Arbeitsabläufe in einer rundum sicheren Umgebung

In Zeiten von On-Premises Netzwerken mit Servern und Systemen an einem Ort waren Netzwerk-Firewalls und VPNs klassische Sicherheitsmodelle zum Schutz der lokalen Infrastruktur. Mit dem Wechsel in die Cloud mit Home-Office und ortsunabhängigem Arbeiten reichen diese Verfahren aber nicht mehr aus, um sich gegen reale Bedrohungen zu schützen.
Mit dem Zero-Trust-Ansatz hat sich eine Sicherheits-Philosophie etabliert, die sich der Komplexität der modernen Umgebung anpasst. Zero-Trust schützt die IT-Infrastruktur, Geräte, Daten, Anwendungen und Mitarbeitende vor Cyber-Attacken und Sicherheitsrisiken, egal wo sie sich befinden.

Microsoft 365 bietet verschiedene Ansatzpunkte, um den digitalen Arbeitsplatz mit diesen Schutzfunktionen auszustatten:

- Erster Ansatzpunkt ist das **Azure Active Directory** (Azure AD), dass eine Identitäts- und Zugriffsverwaltung mit Single-Sign-On und einer sicheren Identifikation sowohl für interne als auch für externe Benutzer in der gesamten digitalen Umgebung gewährleistet.

- Zweiter Ansatzpunkt ist der Verzicht auf **unsichere Passwörter**. Passwörter sind bekanntermaßen eines der größten Sicherheitsprobleme. Selbst starke Passwörter sind anfällig für Angriffe, sei es durch fahrlässigen Umgang durch die Anwender, durch Brute-Force-Attacken oder per E-Mail-Phishing durch Cyber-Kriminelle.

  Die „**kennwortlose Authentifizierung**“ verzichtet auf Passwörter. Die Anwender bestätigen ihre Identität mit einem Mobiltelefon, durch biometrische Sensoren (Fingerabdruck-Scan, Gesichtserkennung) oder eine PIN. Über Technologien wie Windows Hello, die Microsoft Authenticator App für Android und iOS oder separate FIDO2-Hardwaregeräte kann sich der Anwender damit

sicher und einfach authentifizieren, ohne ein Kennwort auf einem Gerät oder in einem Netzwerk speichern zu müssen. Veraltete und unsichere Legacy Authentifizierungsverfahren können und sollten abgeschaltet werden.

- Dritter Ansatzpunkt ist **Azure Active Directory Conditional Access**, das das Prinzip „Zugriff mit den geringsten Rechten" umsetzt. Dabei erhält der Anwender nur die Zugriffsrechte, die im Kontext der konkreten Anforderung möglich sind – so viel wie nötig, so wenig wie möglich.

Übrigens: 98 Prozent aller Cyber-Angriffe lassen sich theoretisch mit einer Sicherheits-Basiskonfiguration abwehren, aber nur 20 Prozent der Microsoft-Kunden verwenden eine starke Multi-Faktor-Authentifizierung (MFA), obwohl sie kostenlos ist und standardmäßig aktiviert werden kann.

Effizienzblocker im Bereich Governance

Microsoft 365 besteht aus einer Vielzahl von Apps und Features. Anwender können sich ihre Arbeitsumgebung passend an ihre Teams, Projekte und individuelle Arbeitsweisen konfigurieren. Damit diese Flexibilität nicht im Chaos endet, braucht es Regeln, Vorgaben und Leitplanken, die ein Governance-Konzept festschreibt. Das Konzept regelt zum Beispiel die Art und Weise, wie Gruppen, Sites und Teams bereitgestellt werden, welche Konventionen für die Bezeichnung von Dokumenten, Bibliotheken, Sites und Teams gelten, welche Vorlagen zur vereinfachten Bereitstellung von Sites und Teams zur Verfügung stehen oder ob und in welchem Umfang eine externe Freigabe von Ressourcen unterstützt wird.

Die Umsetzung der Governance-Regeln erfolgt durch entsprechende Konfigurationen von Microsoft 365, bei denen an vielen Stellen entsprechende Features aktiviert oder deaktiviert werden können.

In Microsoft Teams oder auf OneDrive lassen sich Dokumente sehr einfach mit anderen Mitarbeitenden teilen und gemeinsam bearbeiten. Arbeiten Teams mit externen Personen zusammen, ist es für eine reibungslose Zusammenarbeit sinnvoll, diesen Personen auch Zugriff auf die Ressourcen zu ermöglichen. Unter Umständen birgt das aber Risiken, die aus Unternehmenssicht unerwünscht sind und daher oft eine generelle Blockade von externen Zugriffen nach sich ziehen.

Folgen sind ineffizientes Arbeiten des Teams und der unsichere Versand von Dokumenten über E-Mail. Oftmals suchen sich Mitarbeitende dann auch alternative Lösungen außerhalb von Microsoft 365, Stichwort Schatten-IT. Die wiederum bringt erhebliche zusätzliche Risiken für das Unternehmen mit sich.

Lösungsansatz für die Effizienzsteigerung durch eine smarte Governance-Strategie

Der externe Zugriff auf interne Ressourcen macht die Arbeit in Projekten, an denen externe Personen mitarbeiten, wesentlich effizienter. Alle am Projekt beteiligten Personen haben Zugriff auf die relevanten Informationen.

Es wird aber auch Szenarien geben, in denen vertrauliche und sensible Themen behandelt werden, sodass der externe Zugriff aus Sicherheitsbedenken unerwünscht ist. Insofern ist es sinnvoll, den externen Zugriff nicht generell ab- oder freizuschalten, sondern dies situationsabhängig zu entscheiden. Die Kriterien und Regeln, nach denen im Einzelfall entschieden wird, sind Bestandteil des Governance-Konzepts.

Wichtig ist an dieser Stelle zu betonen, dass es nicht nur um die Frage „Externer Zugriff: Ja oder Nein“ geht. Wie fast alle Features in Microsoft 365 hat auch der externe Zugriff diverse Optionen und Stellschrauben, die individuelle Einstellungen ermöglichen. Wer darf wo Dateien teilen, muss dafür ein Passwort vergeben werden oder nicht, ist nur der Lesezugriff oder auch das Bearbeiten gestattet, gilt die Freigabe unbegrenzt oder erhält sie ein Ablaufdatum – all das sind mögliche Konfigurationen für die Freigabe externer Personen.

Aber: um dieses Feature optimal für das eigene Unternehmen einzurichten, müssen einige Voraussetzungen erfüllt sein:

Die IT-Verantwortlichen müssen das Feature, dessen Konfiguration und die Auswirkungen kennen, beurteilen und in den digitalen Arbeitsplatz implementieren.

Mitarbeitende, die damit arbeiten, müssen Schulungen über Funktionen, Auswirkungen und zur Nutzung erhalten.

Die Nutzung in der Praxis und die Auswirkungen auf die Arbeitsprozesse müssen überwacht werden, um mögliche Fehler und Optimierungspotenziale zu erkennen und entsprechend darauf zu reagieren.

Was hier exemplarisch für den externen Zugriff beschrieben wurde, gilt auch für alle anderen Bereiche in Microsoft 365:
Wer darf neue Teams anlegen? Welche Namenskonventionen gelten für die Benennung der Teams? Welche Bestandteile wie Kanäle, Dateien und Dateiablagen, Konnektoren usw. enthält Teams? Gibt es Vorkonfigurationen für die jeweiligen Bestandteile? Werden Vorlagen bereitgestellt, um jedes neue Teams nicht wieder komplett manuell einrichten zu müssen?

Die Liste der Optionen ist lang – ohne allgemeine Rahmenbedingungen ist das Chaos vorprogrammiert und die Effektivität der Mitarbeitenden wird sinken. Deshalb ist Governance ein entscheidender Faktor bei der erfolgreichen effektiven Umsetzung des digitalen Arbeitsplatzes.

Effizienzblocker im Bereich Compliance

Compliance bedeutet die Einhaltung von Regeln aufgrund gesetzlicher Bestimmungen oder interner Richtlinien durch das Unternehmen und die Mitarbeitenden. Verstöße gegen diese Vorschriften können erhebliche rechtliche, strafrechtliche und finanzielle Folgen für das Unternehmen nach sich ziehen. Unter anderem können sie zu Bußgeldern, Schadenersatzansprüchen oder Verlust von Glaubwürdigkeit und Reputation führen.

Aber auch der versehentliche Datenabfluss beispielsweise durch die automatische Weiterleitung von E-Mails mit oder ohne Anhängen an externe Empfänger stellt ebenfalls ein Sicherheitsrisiko aufgrund der möglichen Veröffentlichung von sensiblen Unternehmensdaten dar.

Lösungsansatz für eine zuverlässige Einhaltung der Compliance-Richtlinien

Um Compliance-Anforderung in und mit Microsoft 365 zu erfüllen, ist zunächst ein Überblick über und ein Verständnis für die Datenlandschaft des Unternehmens erforderlich. Wo werden sensible Daten gespeichert? Für welche Aktionen und Prozesse sind die Daten wichtig? In welchen Formaten (Dokumente, E-Mails, Chatnachrichten, Video- und Audiodateien, Bilder, SharePoint-Listen usw.) sind die Informationen gespeichert?

Sind die kritischen Daten identifiziert, müssen sie kenntlich gemacht und geschützt werden. Dazu klassifiziert man die Daten in einer Taxonomie und erstellt Richtlinien, anhand derer die relevanten Daten erkannt, gekennzeichnet und der Taxonomie zugeordnet werden können. Dies kann manuell durch die User, durch automatische Mustererkennung (z.B. Kreditkartennummern) oder mit Hilfe künstlicher Intelligenz und trainierbaren Modellen erfolgen.

Labels an den Daten kennzeichnen schließlich die Regeln und Policies und geben an, was mit den Daten passieren darf und was nicht.
Microsoft Compliance Funktionen wie **Data Loss Prevention** (DLP) überwachen die Einhaltung dieser Regeln. Sie warnen vor risikoreichem Verhalten oder verhindern z.B. unbeabsichtigte oder fehlerhafte Weitergabe von Daten und Dokumenten, die schützenswerte Informationen enthalten.

Für die Akzeptanz und effiziente Nutzung ist die Integration der Compliance-Funktionen in den digitalen Arbeitsplatz erforderlich und zwar direkt in die jeweilige Applikation oder Anwendung, mit der der Mitarbeitende arbeitet.
Nehmen wir z. B. ein Dokument, das mit dem Label „Kein E-Mailversand“ gekennzeichnet ist. Wird dieses Dokument als Anhang in eine E-Mail eingefügt, erscheint direkt in Outlook ein entsprechender Hinweis und das System blockiert automatisch den Versand der E-Mail bzw. das Anfügen des Dokuments an die E-Mail.

Effizienzblocker im Bereich Infrastruktur

Die Mitarbeitenden arbeiten im Büro, unterwegs oder im Home Office. Sie nutzen eine Vielzahl von firmeneigenen oder privaten Endgeräten mit verschiedenen Betriebssystemen und greifen über externe Netzwerke auf ihren digitalen Arbeitsplatz zu. Diese heterogene Infrastruktur zu managen, damit sie sicher und zuverlässig funktioniert, stellt die Administration vor erhebliche Herausforderungen. Welche Geräte sind im Einsatz, wie werden aktuelle Sicherheitsupdates ausgerollt, welche Apps haben Kompatibilitätsprobleme mit neuen Windows Versionen – diese und viele weitere Aufgaben müssen effizient gelöst werden.

Lösungsansatz für das effiziente Management einer komplexen Infrastruktur

Eine flexible Arbeitsumgebung wie Microsoft 365 geht fast immer auch mit einer heterogenen IT-Infrastruktur einher. Das stellt besondere Anforderung an das Infrastrukturmanagement.

Die Lösung, die Microsoft 365 hier bietet, ist der **Microsoft Endpoint Manager**, eine zentrale Verwaltungsplattform zum Management und zur Überwachung aller Endpunkte im Unternehmen. Endpunkte können Desktops, Server, mobile Endgeräte, Apps, Embedded Systems, holografische Geräte wie die Hololens, Whiteboards und andere Geräte sein.

Zur Verwaltung dieser Systeme integriert der Endpoint Manager mehrere Komponenten unter einer zentralen Oberfläche: **Microsoft Configuration Manager, Microsoft Intune, Desktop Analytics** und **Windows Autopilot**.

Mit dem **Microsoft Configuration Manager** werden Geräte wie PCs, Laptops oder Server verwaltet egal, ob sie sich an einem lokalen oder externen Standort oder als virtuelles System in der Cloud befinden. Über den Configuration Manager können Anwendungen, Softwareupdates, Betriebssysteme bereitgestellt, Geräte in Echtzeit analysiert und überwacht und Compliance-Einstellungen vorgenommen werden. Unterstützt werden Windows- und macOS basierte Systeme.

Microsoft Intune verwaltet cloudbasiert mobile Geräte wie Mobiltelefone oder Tablets (MDM) und mobile Anwendungen (MAM). Mit Intune lassen sich Richtlinien erstellen, die den Zugriff auf Daten und Netzwerke des Unternehmens festlegen, Apps vorkonfigurieren, ausrollen und aktualisieren sowie Nutzungsstatistiken abrufen. Auch Geräte, die nicht mehr benötigt werden oder verloren gegangen sind, lassen sich entfernen und löschen. Microsoft Intune unterstützt Geräte mit iOS, macOS, Android und Windows 10/11.

Desktop Analytics unterstützt den Updateprozess speziell bei Windows-Geräten. Bei Software- oder Treiber-Updates stellt sich stets die Frage, ob die Updates mit den bestehenden Systemen kompatibel sind. Desktop Analytics verwaltet ein Geräte- und Software-Inventar und stellt dafür ein Set von Analysen, Informationen und Tests zur Verfügung, mit denen mögliche Auswirkungen oder Kompatibilitätsprobleme von Updates vorab identifiziert werden können.

Windows Autopilot vereinfacht die Bereitstellung von Windows 10/11 Geräten am Arbeitsplatz. Mit dem Windows Autopilot lassen sich die unternehmens- und arbeitsplatzspezifischen Einstellungen des Betriebssystems so vorkonfigurieren, dass der Mitarbeiter, der das Gerät erstmalig in Betrieb nimmt, automatisch die für ihn optimierte PC-Konfiguration erstellt bekommt. Auch das Zurücksetzen oder Wiederherstellen von Geräten kann über den Windows Autopilot vorgenommen werden.

Effizienzblocker im Bereich Changemanagement

Microsoft 365 bietet den Mitarbeitenden mit seinen Apps und Funktionen vielfältige Möglichkeiten, einen für sich optimal zugeschnittenen digitalen Arbeitsplatz zu gestalten. Fehlt aber das Wissen um die Funktionen und Möglichkeiten des persönlichen digitalen Arbeitsplatzes, haben Mitarbeitende meist auch kein richtiges Verständnis oder Motivation dafür, die Tools für die Zusammenarbeit zu nutzen. In diesen Arbeitssituationen leidet dann die Effizienz der Teams.

Lösungsansatz für Effizienzsteigerung am digitalen Arbeitsplatz durch fachliches Know-how

Microsoft 365 als der digitale Arbeitsplatz ist nur ein Werkzeug. Um damit effizient arbeiten zu können, bedarf es einer bestimmten mentalen Einstellung zur Art und Weise, wie wir arbeiten, die wir ganz allgemein mit „Modern Work" beschreiben. In unserem Whitepaper „Der Digital Workplace mit Microsoft 365" gehen wir ausführlich auf Modern Work, den Dreiklang von Mindset, Skillset, Toolset und damit zusammenhängende Maßnahmen und Empfehlungen des Changemanagements ein.

Das Fazit:

Die Einführung des modernen Arbeitsplatzes erfordert einen ganzheitlichen Ansatz, der Unternehmenskultur, Management, Anwender, IT-Administration und Technik zusammenführt. Neue Verhaltensweisen müssen gelernt und alte entlernt werden.

Um diese Veränderungen von Unternehmenskultur und Arbeitsweisen im Unternehmen in Gang zu bringen und nachhaltig zu etablieren, empfiehlt es sich externe Expertise auf dem Feld von Changemanagement zu holen. Der Blick von außen ist oft hilfreich, um Veränderungsprozesse einfacher und schneller in Bewegung zu bringen als es für unternehmensinterne Personen möglich wäre.

Effizienzblocker im Bereich Geschäftsprozessoptimierung

Microsoft 365 bietet einen umfangreichen Werkzeugkasten für die moderne Arbeit in Projekten und Teams. Dokumente und Daten sind im digital Workplace gespeichert. Die Arbeitsabläufe mit diesen Daten sind oft nicht digitalisiert, sondern werden durch manuelle Interaktion und mit Systembrüchen ausgeführt. Dadurch entstehen Effizienzblocker wie Zeitverlust, Dateninkonsistenz oder Mehrarbeit.

Lösungsansatz für effiziente Automatisierung und Optimierung von Geschäftsprozessen

Um Prozesse zu digitalisieren und automatisieren gab es schon immer Workflow-Lösungen. Die Umsetzung der manuellen Prozesse auf digitale Workflows erforderte aber Programmierkenntnisse, was einer knappen und teuren Ressource entspricht. Deshalb lohnte es sich gerade bei kleinen Arbeitsabläufen oft nicht, diese zu digitalisieren.

Das hat sich mit der **Microsoft Power Plattform** als Teil von Microsoft 365 grundlegend geändert. Mit ihr können Mitarbeitende im Selfservice ihre Abläufe schnell, einfach und kostengünstig automatisieren.

Die Mindestanforderung dafür sind Grundkenntnisse der Plattform mit **PowerAutomate** und **PowerApps** und das Wissen, wie mit diesen Tools Lösungen gebaut werden können. Diese Kenntnisse sind aber mit einem überschaubaren Schulungsaufwand erlernbar.

Aber, wie schon mehrfach erwähnt, bedarf es einem zentral vorgegebenen Rahmen, wer, wo und wie mit der Power Plattform eigene Lösungen erstellen darf. Andernfalls entstehen Chaos und fehlerhafte, nicht mehr nachvollziehbare oder evtl. schädliche Prozesse.

PROBLEMLÖSER VON ARVATO SYSTEMS

Microsoft 365 im Unternehmen effizient und sicher zu betreiben, ist für das einzelne Unternehmen in der Regel mit einem hohen Zeit- und Kostenaufwand verbunden. Wie in diesem Whitepaper verdeutlicht, erfordert insbesondere die Komplexität und Vielfältigkeit der Plattform viel Erfahrung und fundierte technische Kenntnisse.

Deshalb lohnt es sich, bestimmte Aufgaben auf Dienstleistungsunternehmen zu verlagern, die sich auf das Management von Microsoft 365 spezialisiert und entsprechende Expertise aufgebaut haben.

In einer Studie der International Data Group (IDG) aus dem Jahr 2021 gaben rund 97 Prozent der befragten Unternehmen an, dass sie auf die Leistungen von Managed Service Providern zurückgreifen. Das Ziel dieser Unternehmen ist es, durch die externen Serviceleistungen hohe Kostenersparnisse und flexiblere Kostenstrukturen zu erreichen. Arvato Systems wurde im Rahmen dieser Studie als einer der besten Managed Service Provider in der Umsatzklasse 2 (250-1.000 Mio. Jahresumsatz) ausgezeichnet.

Workplace Enterprise Suite für Managed Services (WPES)

Arvato Systems bietet mit der Workplace Enterprise Suite für Managed Services ein Dienstleistungspaket für den technischen Betrieb von Microsoft 365, das die Bereitstellung, Problemlösungen, Aktualisierungen, Monitoring und den allgemeinen Betrieb umfasst.

Mit entsprechendem Know-how und einer langjährigen Praxiserfahrungen aus einer Vielzahl betreuter Kundeninstallationen erstellt Arvato Systems eine individuelle, an die speziellen Anforderungen des Unternehmens angepasste technische und operative Lösung. Sie erhalten damit nicht nur eine effektive Konfiguration der relevanten Services, sondern auch einen wirksamen Schutz im Kampf gegen Cyber-Attacken.
Unternehmensintern bleibt der Fokus dadurch weiterhin auf dem Kerngeschäft. Die eigenen Kräfte haben mehr Zeit, um sich auf die Adoption, das Training und die Unterstützung der Mitarbeitenden beim alltäglichen Einsatz von Microsoft 365 zu konzentrieren.

WPES umfasst verschiedene Services:

- **Tenant Management:** Sie erhalten einen gemanagten Microsoft 365-Tenant, der mit Standardeinstellungen für Apps wie SharePoint, Teams und Exchange eingerichtet wird. Im Rahmen eines Security- und Berechtigungskonzept nimmt Arvato Systems eine Basis-Sicherheits-Konfiguration für alle Identitäten, Geräte und Systeme vor, um die Unternehmensressourcen vor den häufigsten Cyber-Attacken zu schützen.
- **Compliance und Identity Security:** Gemeinsam mit Experten von Arvato Systems erarbeiten Sie Sicherheitsanforderungen für alle Microsoft 365 Dienste. Um die Konfiguration und Administration der erforderlichen Funktionen müssen Sie sich nicht mehr kümmern.
- **User- und Access Management:** Als Benutzer erhalten Sie die Möglichkeit, Ihre Passwörter selbst zu verwalten und zurückzusetzen. Sie haben Zugriff auf Support-Dokumente und managen Ihre Microsoft 365 Lizenzen mit Unterstützung von Arvato Systems.

- **E-Mail- und Client-Security:** Mit dem Microsoft Defender for Endpoint werden Technologien wie Endpoint Verhaltenssensoren, Threat Intelligence und Analyse der Cloud-Sicherheit eingesetzt, um mögliche Bedrohungen durch E-Mail-Attacken oder Angriffe auf Endgeräte zu erkennen und abzuwehren.
- **Device Management:** Sie erhalten einen Windows Basis-Client als IT-Arbeitsplatz, der mit dem Windows Autopilot eingerichtet, vorkonfiguriert und mit einem Standard-Software-Paket ausgestattet ist. Mit der Remote Wipe-Funktion für das Basis-Image lassen sich innerhalb kurzer Zeit verloren gegangene Geräte aus der Ferne löschen, sodass keine Daten in die falschen Hände gelangen können.
- **Managed Detection & Response:** Managed Services beinhalten ein fortlaufendes Security-Monitoring, mit dem mögliche sicherheitskritische Ereignisse erkannt und bewertet werden. Arvato Systems analysiert und priorisiert relevante Ereignisse im Hinblick auf potenzielle Auswirkungen und reagiert mit entsprechenden Reaktionen und Gegenmaßnahmen darauf.
- **Collaboration Management:** Je nach Kundenwunsch werden auch die Microsoft 365 Kollaborationslösungen wie Exchange Online, OneDrive for Business Online, SharePoint Online oder Teams (Standard) konfiguriert und verwaltet.

NAVOO

Speziell für Ihre IT-Governance und die Anpassung der Microsoft 365 Standardumgebung an die individuellen Anforderungen des Unternehmens bietet Arvato Systems mit NAVOO eine umfangreiche und smarte Lösung für den Digital Workplace an.

NAVOO erweitert die Standardfunktionen von Microsoft 365 um Customer Templates, Vorlagen für Intranet, Content Lifecycle und Security, zusätzlichen Apps und Webparts, angepassten Such- und Newsseiten, Governance- und Self-Service-Funktionen und vielen weiteren Bausteinen.

Mehr zu **NAVOO** und Herausforderungen rund um das Changemanagement lesen Sie im **Whitepaper „Der Digital Workplace mit Microsoft 365".** Hier finden Sie Tipps für die erfolgreiche Einführung eines digital Workplace und praktischen Checklisten für IT-Administratoren zur Unterstützung der Anwender und zur Auswahl von Tools.

» Jetzt kostenlos lesen

Checkliste: Anforderungen an das Know-how und Aufgaben in Microsoft 365

- Ich muss wissen, dass es ein Feature gibt und welchen Zweck es erfüllt.
- Ich muss wissen, wie das Feature funktioniert, wie es konfiguriert wird, wie die Mitarbeitenden es in der Praxis einsetzen können und welche Auswirkungen es auf die Arbeitsweise hat.
- Ich muss das Feature an die Anforderungen meines Unternehmens anpassen und es entsprechend konfigurieren.
- Die Anwender müssen das Feature verstehen und damit umgehen können, daher muss der Roll-Out durch entsprechende Information und gegebenenfalls Trainings begleitet werden.
- Ich muss die Effektivität, Wirksamkeit und Sicherheit in der täglichen Anwendung überwachen können und gegebenenfalls Anpassungen vornehmen oder auf Abweichungen proaktiv reagieren.
- Ich muss die Entwicklung des Features monitoren. Wenn Microsoft Änderungen an einem Feature, der Benutzeroberfläche oder an den einzelnen Funktionen vornimmt, muss ich die Auswirkungen auf meine individuelle Konfiguration und die Anwendung in meinem Unternehmen beurteilen und entsprechend reagieren.
- Und in einer komplexen Umgebung wie Microsoft 365 können Änderungen an einem Feature Auswirkungen auf andere Funktionen oder auch Arbeitsabläufe haben. Auch darauf muss ich achten.

FAZIT UND AUSBLICK

Grundvoraussetzung für einen effizienten Betrieb von Microsoft 365 ist ein umfassendes, an die spezifischen Anforderungen des Unternehmens angepasstes Betriebskonzept für Sicherheit, Governance, Compliance, Infrastruktur und Benutzererfahrungen.

Microsoft 365 ist ein komplexes System, dessen Management ein hohes Maß an Kenntnissen, Erfahrungen und Zeit erfordert, um die Möglichkeiten der Plattform effizient und sicher zu nutzen. Dies sollte man auf keinen Fall unterschätzen. Ob und inwieweit sich das Know-how und die personellen Ressourcen dafür im Unternehmen selbst aufbauen lassen, muss man im Einzelfall prüfen.

Angebote wie Workplace Enterprise Suite für Managed Services können eine gute und auch kostengünstige Alternative dazu sein. Das Unternehmen kann auf das Fachwissen bei Arvato Systems durch die Erfahrungen und Best-Practice aus einer Vielzahl von betreuten Kunden-Systemen zurückgreifen. Bei Problemen, Anpassungen und Erweiterungen bietet Arvato Systems qualifizierte Beratung und Unterstützung auf Augenhöhe.

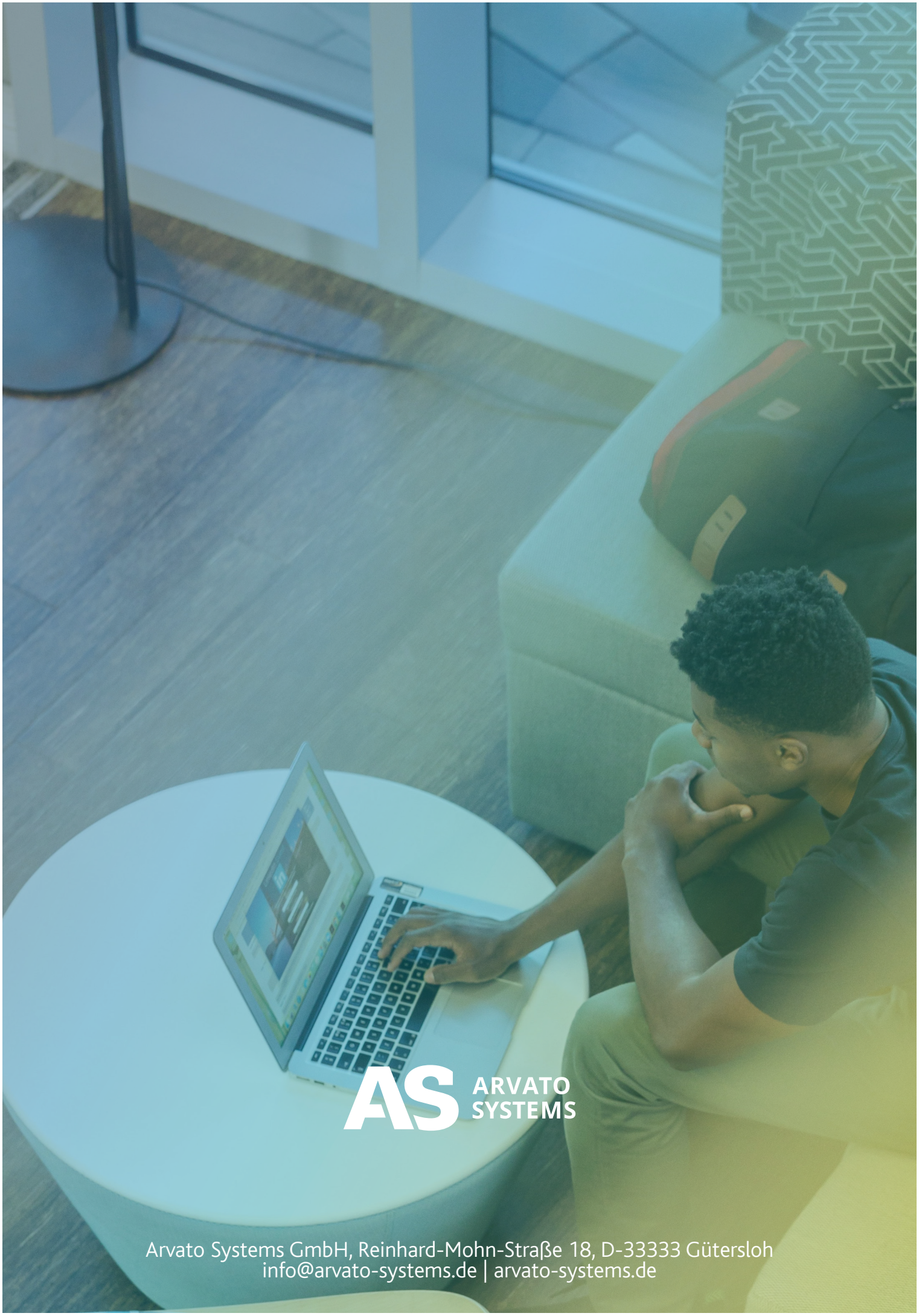
Start

Kontakt

Sie haben Fragen zum Digital Workplace,
zum Whitepaper oder zu NAVOO? Melden Sie sich gerne bei uns!

Tim Seebrandt
Customer Success Manager
Phone: +49 (5241) 80-79491
E-Mail: tim.seebrandtf@bertelsmann.de

www.navoo.com



Arvato Systems GmbH, Reinhard-Mohn-Straße 18, D-33333 Gütersloh
info@arvato-systems.de | arvato-systems.de