Arvato Systems Whitepaper

Gast User Management für mehr Sicherheit und Kontrolle

Ihr Guide für eine effiziente und sichere Zusammenarbeit mit externen Personen

ARVATO SYSTEMS

START

EINLEITUNG

Die Zusammenarbeit mit Gastbenutzer:innen ist für den Erfolg eines Unternehmens essentiell, aber auch schnell unübersichtlich und dadurch risikobehaftet. Studien zeigen die Probleme, die mit fehlerhaft konfigurierten Identitäten in Unternehmen entstehen. So gibt die Identity Defined Security Alliance (IDSA) beispielsweise an, dass 79 Prozent der Unternehmen in den letzten zwei Jahren eine Sicherheitsverletzung im Zusammenhang mit Identitäten erlebt haben. Die Cybersicherheitsforscherin und ehemalige Hackerin Alissa Knight sagt dazu, dass sie sofort nach Rechten sucht, wenn sie eine Lücke im Netzwerk gefunden hat. Dafür reicht es, die Anmeldeinformationen aus den Systemspeichern auszulesen.

Demnach spielt ein optimales Gast User Management – also die sichere Verwaltung von Gastbenutzer:innen in Infrastrukturen und Cloud-Plattformen wie Microsoft 365-Umgebungen – eine wichtige Rolle.

Gleichzeitig sind Sie als Unternehmen auf den Austausch mit externen Nutzer:innen angewiesen. Dabei gibt es viele Einsatzgebiete, die den Einsatz von Gastkonten notwendig machen. Externe Mitarbeitende, wie Partner:innen und Lieferant:innen beispielsweise, müssen oft mit internen Mitarbeitenden auf gemeinsame Ressourcen und Dokumente zugreifen und an Besprechungen teilnehmen, wie in Microsoft Teams.

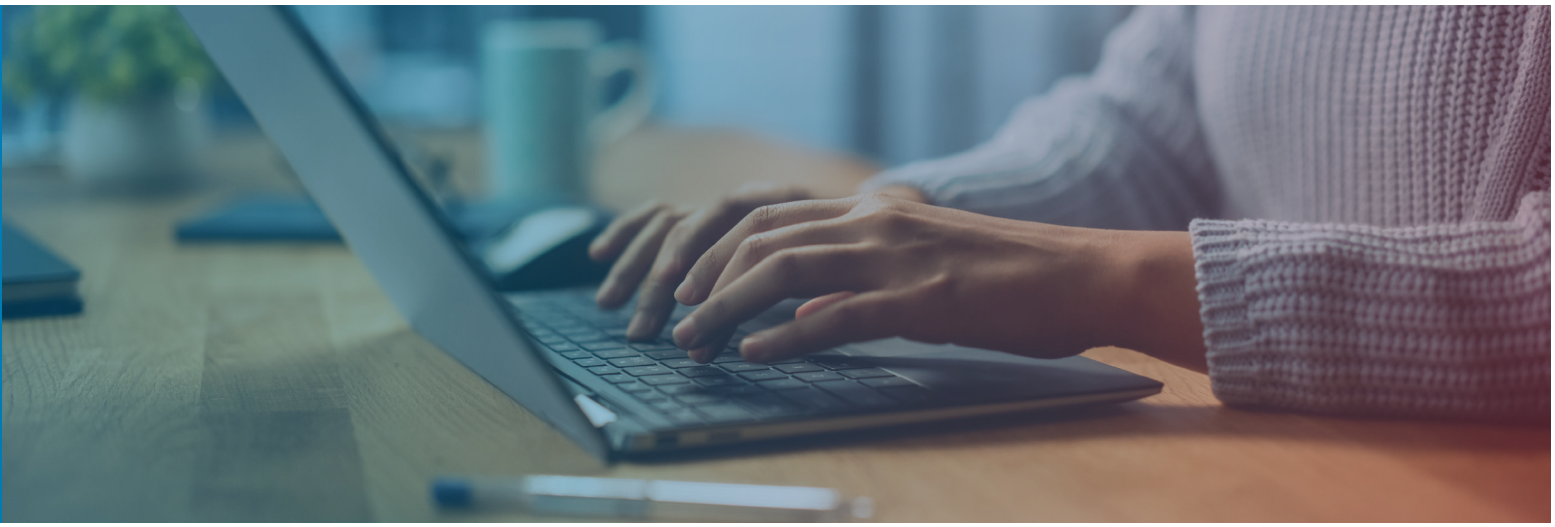
In diesem Whitepaper betrachten wir Relevanz, Chancen, Herausforderungen und Lösungen des Gast User Managements. Wir zeigen Ihnen, worauf Sie beim Einsatz und der Verwaltung von Gastkonten achten müssen und wie Sie potenzielle Gefahrenquellen minimieren, ohne den Nutzen zu stark einzuschränken. Erfahren Sie, welche Rechte Gastkonten benötigen und warum Sie inaktive Gastkonten wieder aus der Umgebung löschen sollten.

GASTKONTEN SPIELEN EINE WICHTIGE ROLLE FÜR DEN UNTERNEHMENSERFOLG

Für eine effektive Zusammenarbeit sind Gastkonten unerlässlich, da Projekt-Teams oder Prozesse im Unternehmen oft von externen Partnerschaften abhängen. Eine digitale Kooperation mit externen Personen erhöht die Produktivität der eigenen Mitarbeitenden und verschafft Ihrem Unternehmen einen Wettbewerbsvorteil. Dabei spielen die richtige Balance zwischen Benutzerfreundlichkeit und Sicherheit eine große Rolle. Fundiertes Wissen über die beiden Varianten von Gastkonten stellt sicher, dass Sie diese korrekt einsetzen und absichern:

I. Variante: Gastbenutzer:innen (Gast User)

Gastbenutzer:innen erhalten in Microsoft 365 personalisierten Zugriff auf bestimmte Gruppen, Teams, Dokumente sowie andere Ressourcen und können so mit internen Nutzer:innen zusammenarbeiten. Dazu müssen Ihnen die Mitarbeitenden Zugriff auf die jeweiligen Unterhaltungen, Dokumente und Daten in Microsoft Teams, SharePoint oder OneDrive gewähren. Sofern noch keine Regulierung etabliert wurde, können Gastbenutzer:innen von allen Mitarbeitenden durch die Eingabe der einzuladenden E-Mail-Adresse angelegt werden.



II. Variante: Externe Benutzer:innen (External User)

Gastbenutzer:innen erhalten in Microsoft 365 personalisierten Zugriff auf bestimmte Gruppen, Teams, Dokumente sowie andere Ressourcen und können so mit internen Nutzer:innen zusammenarbeiten. Dazu müssen Ihnen die Mitarbeitenden Zugriff auf die jeweiligen Unterhaltungen, Dokumente und Daten in Microsoft Teams, SharePoint oder OneDrive gewähren. Sofern noch keine Regulierung etabliert wurde, können Gastbenutzer:innen von allen Mitarbeitenden durch die Eingabe der einzuladenden E-Mail-Adresse angelegt werden.

Bei Gastbenutzer:innen steuern Sie hingegen individuell den Zugriff einzelner Benutzer:innen und behalten so die Kontrolle über die Zugriffe der einzelnen Konten.

Schlussendlich machen Sie es Ihren Mitarbeitenden sehr einfach, Daten mit den Mitarbeitenden des Partnerunternehmens zu teilen. Beim Einsatz von „Shared Channels“ geben Sie den externen Benutzer:innen einen Freifahrtschein für den Zugriff auf Ihre Daten. Betrachten Sie diese Variante kritisch und setzten Sie diese nur im Ausnahmefall ein. Generell gilt: Verantwortliche müssen Sorgfalt walten lassen, bevor Sie Gast Usern Zugriff gewähren.

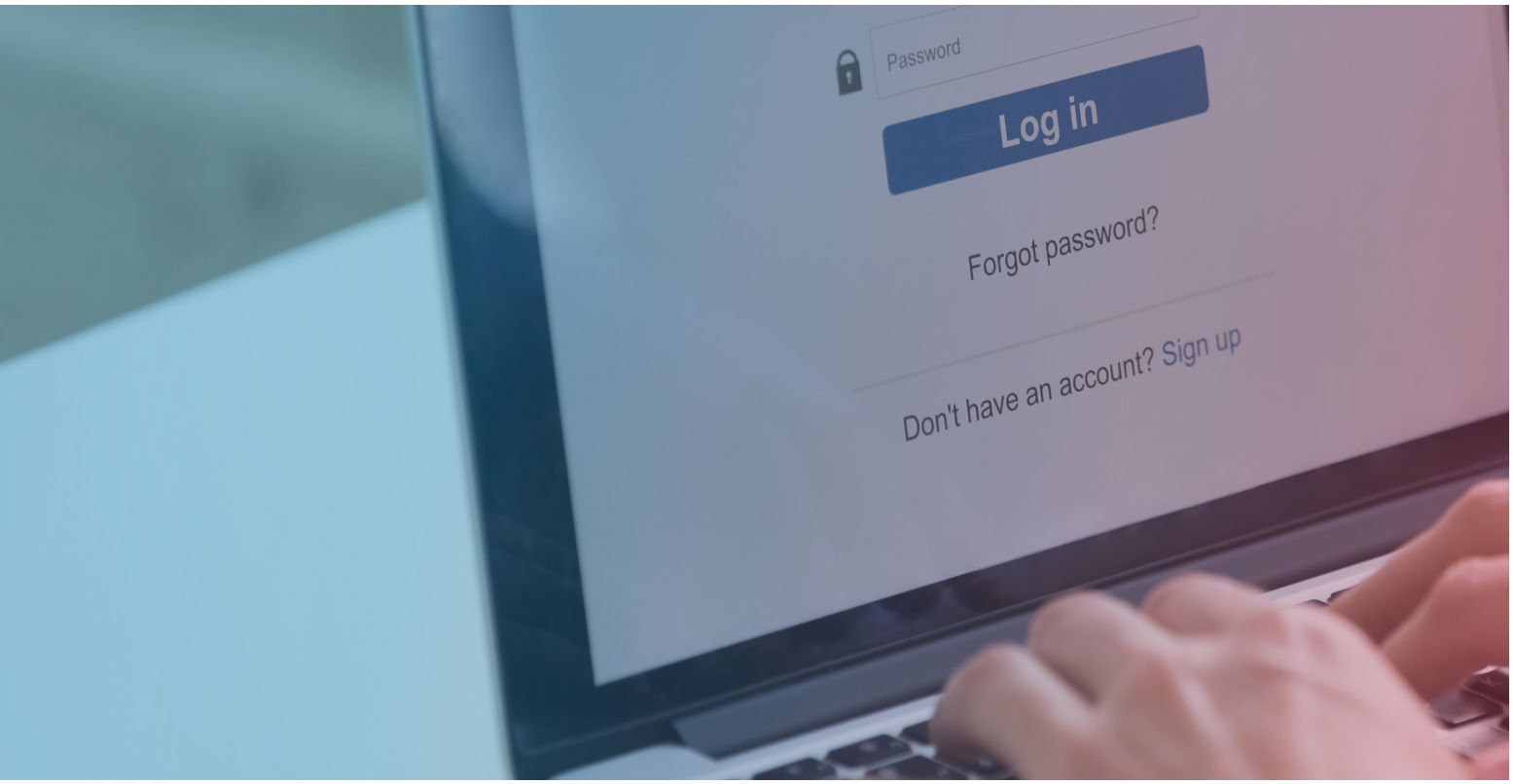
External Users kommen jedoch häufig zum Einsatz, wenn ein Unternehmen Tochterunternehmen anbinden möchte. Hier ist das Grundvertrauen von Natur aus größer als bei externen Unternehmen, die eigene Interessen verfolgen und auf deren IT-Infrastruktur Sie keinerlei Einfluss haben.

In diesem Whitepaper vermitteln wir Ihnen das notwendige Wissen, um den Einsatz von External Users zu vermeiden und dafür auf Gastkonten zu setzen, bei denen Sie vollständig die Kontrolle behalten.

MICROSOFT 365 GAST ACCESS: MÖGLICHKEITEN UND SICHERHEITSLÜCKEN

Microsoft 365 bietet viele Möglichkeiten für das gemeinsame Arbeiten in der Cloud an Ressourcen, Dokumenten und Daten. Kommunikation und Datenaustausch zwischen Teammitgliedern sind in Microsoft 365 einfach möglich – denn Microsoft 365 ist auf eine effektive Zusammenarbeit zwischen Teams ausgelegt.

Die Authentifizierung erfolgt über Azure Active Directory und bietet an dieser Stelle zahlreiche Sicherheitsfunktionen, eine Multifaktor-Authentifizierung und Kontrolle der Benutzer:innen. Gleichzeitig können berechtigte Personen zusätzlich Gäste einbinden, indem sie diese über ihre eigene E-Mail-Adresse einladen, zum Beispiel in Microsoft Teams. Dadurch erhalten Gäste sofort einen kontrollierten Zugriff auf alle Ressourcen des Teams und die öffentlichen Kanäle.



Indem Admins die Zugriffe und Berechtigungen der Gastnutzer:innen richtig steuern, vermeiden Sie das Risiko einer Schatten-IT. Diese kann zum Problem werden, da sie ohne Wissen der IT-Abteilung in den Fachabteilungen von Unternehmen zum Einsatz kommt. Dementsprechend ist eine Schatten-IT kaum vor Cyber-Angriffen geschützt. Mit einem effizienten Gast User Management sorgen Sie für eine sichere sowie effektive Zusammenarbeit und geben einer Schatten-IT keinen Raum.

Ob eine Zusammenarbeit mit Gastkonten (noch) erforderlich ist, kann die IT-Abteilung allerdings kaum bewerten. Das fällt in den Aufgabenbereich der fachlichen Verantwortlichen in den einzelnen Abteilungen. Die IT kann lediglich feststellen, dass sich Gäste längere Zeit nicht angemeldet haben, und die fachlichen Verantwortlichen darauf hinweisen. Zudem kann die IT automatisierte Ablaufzeiten für die Konten festlegen.

Das Gast User Management ergänzt Microsoft 365 optimal

Mit einem Gast User Management können die fachlichen Verantwortlichen selbst Gäste in Teams einladen und sicher verwalten. Die notwendigen Richtlinien und Einstellungen sowie die Überwachung erfolgen dabei durch ein effektives Gast User Management-System, das die Einladung der Gast User unter kontrollierten Bedingungen unterstützt.

Benötigen Sie bestimmte Gastkonten nicht mehr, sollten Sie diese deaktivieren oder löschen – abhängig davon, welche Richtlinien für Ihre Organisation gelten.

Dadurch erhalten Sie eine nachhaltige Kontrolle über Gastzugriffe bei maximaler Produktivität der Benutzer:innen. Gleichzeitig gewährleistet ein Gast User Management durch die automatisierte Verwaltung sowie Überwachung der Gastkonten eine effektive Cybersicherheit.

FOLGEN EINES UNZUREICHENDEN GAST USER MANAGEMENTS

So vorteilhaft die Zusammenarbeit über Gastkonten auch ist, wenn Sie diese nicht kontrollieren, drohen verschiedene Sicherheitsrisiken. Über Gastkonten haben externe Benutzer:innen Zugriff auf die Infrastruktur und Clouddienste eines Unternehmens sowie den darin gespeicherten Daten. Ein Problem dabei ist: Bei der Erstellung von Gastkonten kommt es oft zum sogenannten Over-Sharing – dem übermäßigen Teilen von Daten. Das bedeutet, dass Gäste Zugriff auf Inhalte haben, die für sie irrelevant sind. Der Grund dafür ist, dass es für Mitarbeitende oft einfacher und schneller ist, Rechte im Übermaß zu erteilen, als diese korrekt zu vergeben.

Fallen diese Rechte in die falschen Hände, können schwerwiegende negative Konsequenzen folgen. Diese negativen Folgen sollten Verantwortliche in jedem Fall vermeiden. Nachfolgend sind einige Beispiele aufgeführt:

Das Teilen von sensiblen Daten und daraus resultierende negative Folgen

Oft teilen Mitarbeitende unbedacht sensible Daten mit Gästen. In den meisten Fällen ist es weder notwendig noch erwünscht, dass externe Benutzer:innen darauf Zugriff haben. Das birgt Risiken, die nicht zu unterschätzen sind. Treffen Sie vorbeugende Maßnahmen, um daraus resultierende negative Folgen wie finanzielle Strafen, Kundenabwanderung und Imageverlust zu vermeiden.

Gefahren durch Cyber-Angriffe

Die Vergabe von Gastkonten verläuft unkontrolliert und die Konten der Gast User bleiben oft dauerhaft aktiv – das erschwert die Übersichtlichkeit der vorhandenen Benutzerkonten und bietet Cyberkriminellen eine Angriffsfläche. Sie erhalten leicht Zugriff auf Anmeldeinformationen und damit Zugang zum internen System eines Unternehmens.

Laut dem Verizon Data Breach Incident Report sind Anmeldedaten mit über 60 Prozent die begehrteste Datenkategorie bei Sicherheitsverletzungen. Cyberkriminelle haben leichtes Spiel, indem sie sich einfach mit erbeuteten Benutzerkonten anmelden. Ohne Identitätsrisikomanagement (Identity Risk Management) sind solche Zugriffe jederzeit möglich.

Mit der Anzahl an Benutzerkonten steigt auch die Komplexität der Berechtigungsstrukturen in einem Netzwerk an. Gleichzeitig erhöht sich die Anzahl an potenziellen Sicherheitslücken, die mit den Konten einhergehen.

Meldet sich ein Angreifer in einem nicht mehr benötigten Gastkonto an, kann er nahezu unbemerkt im internen Unternehmensnetzwerk agieren. Aus diesem Grund sollten Sie nicht mehr benötigte Gastkonten so schnell wie möglich deaktivieren oder löschen. Ein Gast User Management-System kann diese Aufgaben standardisieren und automatisieren.

Angriffe von Cyberkriminellen nehmen zu

Eine weltweit durchgeführte Umfrage aus dem Jahr 2022 ergab, dass rund 46 Prozent der befragten Unternehmen in Deutschland mindestens einmal Opfer einer Cyber-Attacke waren. Im Durchschnitt gaben rund 49 Prozent der befragten Firmen aus verschiedenen Ländern an, in den letzten 12 Monaten mindestens einen Cyber-Angriff erlebt zu haben. Deutschland ist zusammen mit den USA am stärksten betroffen.

Schlecht verwaltete Tools bieten ebenfalls eine Angriffsfläche für Cyberkriminelle. Nach Gartner sind "viele Datenschutzverletzungen durch Sicherheits- und Identity-Tools verursacht, die fehlerhaft oder unvollständig konfiguriert wurden oder deren Konfiguration veraltet ist" (Gartner, Predicts 2022). Im schlimmsten Fall fühlt sich keiner der Mitarbeitenden mehr für die Gastbenutzer:innen verantwortlich oder niemand weiß mehr, wer Zugriff hat.

Zudem unterschätzen viele Unternehmen die Anzahl der Gast User in Ihrem Azure AD, weil ihnen nicht bekannt ist, auf welchen Wegen Gastkonten entstehen. Neben der Einladung in ein Microsoft-Teams entsteht ein Gastkonto auch, wenn Mitarbeitende Dateien oder Ordner in OneDrive oder SharePoint freigeben. Eine direkte Einladung in den zentralen Identitätsdienst Azure Active Directory führt ebenfalls zu Gastkonten. Gast Usern wird so der Zugriff auf Tools außerhalb von Microsoft 365 ermöglicht. Diese Remotezugangsdaten sind heutzutage ein begehrtes Handelsobjekt in einschlägigen Internetforen und öffnen Cyberkriminellen die Tür.

Gefahren durch Ransomware-Angriffe

Ineffektiv verwaltete oder unkontrollierte Gastkonten können ebenfalls Ransomware-Angriffe verursachen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt und zieht für 2021 eine negative Bilanz: „Das vergangene Jahr war geprägt von einer deutlichen Ausweitung cyberkrimineller Erpressungsmethoden. Nicht nur die Anzahl der Schadprogramm-Varianten stieg zeitweise rasant an – mit bis zu 553.000 neuen Varianten pro Tag der höchste jemals gemessene Wert. (...) Auch die Qualität der Angriffe nahm weiterhin beträchtlich zu." Im Jahr 2021 sind laut dem „Cyber Attack Trends Mid Year Report 2021" die Angriffe mit Ransomware um 93 Prozent gestiegen. Auch im darauffolgenden Jahr nehmen Cyberangriffe weltweit drastisch zu: „In the first half of the year [2022], there was a 42 Percent increase in weekly cyberattacks globally with every region experiencing a significant escalation."

Dazu trägt die wachsende Anzahl an Gastkonten bei – ein Resultat der Digitalisierung und der damit einhergehenden mobilen Arbeit. So finden immer mehr Besprechungen online statt, bei denen externe Personen Zugriff auf interne Unternehmensressourcen erhalten. Dabei kann es sich um eine Präsentation oder sensible Dokumente handeln, die im Chat einer Videokonferenz geteilt werden. Gleichzeitig ist es für Mitarbeitende oft sehr einfach, Gast User anzulegen, damit sich diese in eine Videokonferenz einwählen können.

Effizienzverlust in der Zusammenarbeit

Die Deaktivierung des externen Zugriffs von Gastkonten ist dabei jedoch nicht zielführend. Damit tragen Sie zwar zu einer erhöhten Sicherheit bei, gleichzeitig erschweren Sie jedoch Mitarbeitenden die effektive Zusammenarbeit mit externen Personen. Die Vorteile, die Microsoft 365 in diesem Zusammenhang bietet, können nur bedingt ausgeschöpft werden.

Doch auch die Sicherheit ist damit langfristig nicht gewährleistet. Im Gegenteil: Ihre Mitarbeitenden müssen und werden andere Wege finden, dennoch mit externen Benutzer:innen zu kommunizieren und Daten auszutauschen. Diese Vorgehensweise begünstigt eine Schatten-IT, die sich meist komplett dem Zugriff Ihrer IT-Abteilung entzieht.

In einer Studie des Cybersecurity-Spezialisten Forcepoint gaben 63 Prozent der Befragten an, mit privaten Endgeräten auf Dokumente und Dienste ihres Arbeitgebers zuzugreifen. Über die Hälfte speichern oder übertragen Arbeitsdaten auf persönlichen USB-Sticks und nutzen private E-Mail- oder File-Sharing-Cloud-Dienste für Arbeitszwecke.

Die Gründe dafür sind eindeutig: Viele Unternehmen bieten ihren Mitarbeitenden keine ausreichenden Möglichkeiten, mit Gästen zu kommunizieren, oder erschweren dies durch strenge Richtlinien. Auch diese Vorgehensweise öffnet die Tür für Malware, Ransomware und Cyberangriffe.

DIE GRÖSSTEN HERAUSFORDERUNGEN IM ÜBERBLICK

Viele Gastbenutzer:innen gleichzeitig sicher und übersichtlich zu managen, ist mit Herausforderungen verbunden, die in der Regel nur spezielle Tools meistern können:

Hohe Anforderungen beim Onboarding von Gastbenutzer:innen erfüllen

Vor allem große Unternehmen unterliegen strengen gesetzlichen Anforderungen und Richtlinien in Bezug auf den externen Zugriff auf Daten und interne Ressourcen durch Gastkonten. Die Einhaltung erfolgt oftmals auf Basis der Compliance. In vielen Fällen setzen Unternehmen dabei auf den Helpdesk, der Gastkonten anlegen und verwalten muss. Das reduziert das Risiko, dass zu viele Personen in einem Unternehmen das Recht erhalten, Gastbenutzer:innen anzulegen. Allerdings wird dadurch die Belastung des Helpdesk deutlich erhöht und die Prozesslaufzeit verlängert.

Das Lifecycle Management für Gast User optimal planen

Der Lebenszyklus von Gast Usern und die dazugehörigen Berechtigungen unterscheiden sich stark von herkömmlichen Benutzerkonten. So kann es beispielsweise deutliche Unterschiede beim Löschen von Berechtigungen oder dem eigentlichen Login geben. Die richtige Planung eines effizienten Lifecycle Managements für Gast User kann Unternehmen dabei vor Herausforderungen stellen. Daraus lässt sich schließen: Eine sorgfältige Planung des Lifecycle Managements im Voraus ist entscheidend – Sicherheitslücken und Datenverluste können so vermieden werden.

Die Übersicht behalten und Gast User effizient und sicher managen

Insbesondere bei kleinen Unternehmen ist zu beobachten, dass mehr Gast User als Mitarbeitende im System hinterlegt sind. Das stellt die Verwaltung vor Herausforderungen und birgt Gefahren für das interne Unternehmensnetzwerk. Die große Anzahl an Gastkonten bringt langfristig mehr unnötige Konten hervor als produktiv notwendige Benutzer:innen.

Das resultiert in den bereits erwähnten Sicherheitsproblematiken, die auch kleine Unternehmen vor große Herausforderungen stellen. Gerade hier kommt es durch mangelnde Kontrolle oft vor, dass Gastbenutzer:innen im Sinne des Over-Sharings zu viele Rechte erhalten und ohne Einschränkung nahezu von überall aus Zugriff auf die Ressourcen des Unternehmens erhalten. Bei nicht korrekt gesetzten Einstellungen für Gastkonten besteht darüber hinaus die Gefahr, dass Gastnutzer:innen Sicherheitsoptionen nutzen können, die für sie nicht vorgesehen sind.

Damit Sie die Übersicht über Gastkonten behalten, müssen Sie intern einen Mitarbeitenden finden, der die Rolle des fachlichen Entscheidenden und das Management der Gastnutzer:innen übernimmt. Zu den schwierigen Aufgaben dieses Mitarbeitenden gehört ebenso die Entscheidung, ob die Zusammenarbeit mit Gästen noch besteht und ob diese noch ein Konto benötigen.

SO GELINGT OPTIMALES GAST USER MANAGEMENT: GASTKONTEN RICHTIG UND SICHER EINSETZEN

Vertrauen ist gut, Kontrolle ist besser. Sie müssen wissen: Welche Gastkonten kommen zum Einsatz? Welche internen Mitarbeitenden haben externe Gast User eingeladen? Auf welche Ressourcen haben sie Zugriff? Und darüber hinaus müssen Sie festlegen, wer Gastkosten anlegen und nutzen darf. Hierbei hilft Ihnen das Gast User Management.

Wir verraten Ihnen, welche Möglichkeiten Sie bei der Verwendung von Gastkonten haben und wie Sie diese Gastkonten gefahrlos einsetzen. Dabei gehen wir auf die richtige Verwaltung der Gastkonten ein und zeigen, wie Sie für diese ein optimales Lifecycle-Management aufbauen können.

Onboarding-Prozesse mit Gast User Management-Systemen

Durch den Einsatz eines Gast User Management-Systems können Sie Onboarding-Prozesse für Gastbenutzer:innen standardisieren und die genannten Herausforderungen meistern.

Im Rahmen der Onboarding-Prozesse ist es möglich zu definieren, welche Informationen Sie von externen Personen benötigen, um ein Konto anzulegen.

Wenn Sie ein Gastkonto anlegen, verschickt das System automatisch eine E-Mail an den Gast, die idealerweise personalisierbar ist. So können Sie beispielsweise über Rechte und Pflichten aufklären, das Design anpassen und Logos sowie eigene Texte und Legal Statements hinzufügen. Das System sollte auch Disclaimer platzieren und Bestätigungen einholen können.

Besonders wichtig ist eine Auditierung der Aktionen, wenn ein Gastkonto angelegt wird. Über Protokolle des Gast User Managements lässt sich so jederzeit feststellen, wer Konten wann erstellt, angepasst und zugewiesen hat. Sie sollten zusätzlich eine Auskunft über die letzte Anmeldung, das Ablaufdatum und den Einsatzort des Gastkontos geben können.

Neben dem vollständigen Löschen eines Gastkontos, muss ein Gast User Management die Möglichkeit bieten, Konten erstmal temporär zu deaktivieren und nach einem weiteren Zeitraum zu löschen. Dadurch bleiben die Berechtigungen erhalten und müssen bei zukünftiger Aktivierung nicht erneut gesetzt werden. Damit das Löschen eines Gastkontos nicht zu früh stattfindet, verschickt das System nach fest definierten Zeiträumen Benachrichtigungen an den Gast und den verantwortlichen Mitarbeitenden in der Fachabteilung.

Professionalisierung des Gast User Managements

Standardmäßig werden in Microsoft 365 nur E-Mail-Adressen von Gastbenutzer:innen erfasst. In vielen Fällen ist das allerdings nicht ausreichend.

Ein durchdachtes Gast User Management-System erfasst weitere wichtige Daten, zum Beispiel:

- Name,
- Adresse,
- Unternehmen,
- Kontaktinformationen und
- die Verantwortlichen.

Aufgrund der erweiterten Datenerfassung kann jedes Gastkonto einer bestimmten Person in einer Fachabteilung zugeordnet und der Zweck des Kontos eindeutig festgelegt werden. Bei Kontrollen durch die IT-Abteilung lässt sich so jedes Gastkonto zweifelsfrei zuweisen, was nicht nur sicherer ist, sondern auch Zeit und Kosten spart.

Ein weiterer Vorteil: Automatisierte Ablaufzeiten lassen sich bereits beim Erstellen des Kontos hinterlegen. Das ist mit den Bordmitteln in Microsoft 365 nicht möglich, stellt aber eine wichtige Funktion dar, damit Sie den Überblick über Gastkonten behalten. Vor dem Ablauf erinnert das Gast User Management beide Seiten – die Verantwortlichen und die Gastbenutzer:innen – daran, dass das Benutzerkonto zu einem bestimmten Zeitpunkt deaktiviert wird.

Analyse von vorhandenen Gastkonten und Zugriffssteuerung

Darüber hinaus kann ein Gast User Management-System die vorhandenen Gastkonten analysieren und Ihnen dabei helfen, die Zugriffe und damit die notwendigen Rechte in Microsoft 365 zu steuern. So verhindert das System beispielsweise, dass Gastkonten mehr Rechte erhalten als sie benötigen. Besitzt das System Filter für verschiedene Zugriffe auf Ressourcen, erleichtert das die Analyse und Steuerung der Gastkonten erheblich.

Analysen von vorhandenen Gastkonten lassen sich auch wie folgt durchführen: Besitzer:innen von Teams und SharePoint-Bibliotheken erhalten eine Aufforderung, die Berechtigungen von Gastkonten in den von ihnen verantworteten Bereichen in regelmäßigen Abständen zu überprüfen. Diese Vorgehensweise stellt sicher, dass fachliche Verantwortliche relevante Informationen über den Ablauf von Benutzerkonten erhalten. Dann können sie entscheiden, ob bestimmte Gastkonten verlängert werden oder nicht.

Automatisierte Abläufe für mehr Sicherheit

Lösungen, die Prozesse weitgehend automatisieren, entlasten den Helpdesk und sorgen gleichzeitig für mehr Sicherheit. Im Helpdesk können Mitarbeitende Fehler machen, ohne dass dadurch Sicherheitslücken auftreten. Ein speziell geschulter Helpdesk ist in diesem Fall nicht notwendig, da ein smartes Tool problemlos potenzielle Fehler beim Anlegen von Benutzerkonten ausschließt.

Temporär verfügbare Gastkonten / Berechtigungen

Gast User Management-Systeme können Gastkonten temporär anlegen, nach der Nutzung deaktivieren oder automatisch löschen und dabei Verantwortliche im Unternehmen einbinden. Dauerhaft aktive Konten, die für Ihr Unternehmen keine Verwendung haben, gehören damit der Vergangenheit an.

Beenden externe Benutzer:innen die Arbeit für ein Unternehmen, ihr Gastkonto ist aber noch aktiv, kann die Person weiterhin auf die Ressourcen des Teams zugreifen. Darüber hinaus ist das Konto ein potenzielles Sicherheitsrisiko für Ihr Unternehmen, da Angreifer:innen das Gastkonto für eine

unberechtigte Anmeldung nutzen können. Ein Gast User Management-System minimiert diese Gefahr, indem es nicht mehr benötigte Konten automatisch deaktiviert und bei Bedarf löscht.

Sicherheitsstandards von Microsoft unterstützen Gast User Management-Systeme

Natürlich ist es auch möglich, dass Sicherheitsstandards von Microsoft das Gast User Management-System unterstützen. Die Standardtools von Microsoft verhindern bei Bedarf, dass Mitarbeitende Screenshots erstellen und Dokumente ausdrucken oder weiterleiten.

Darüber hinaus sollten Sie die Multifaktor-Authentifizierung (MFA) von Gastkonten konfigurieren und überwachen. In komplexeren Umgebungen ist es möglich, dass die MFA nur für den Zugriff von bestimmten Gastkonten oder Ressourcen notwendig ist.

Hinzu kommen Möglichkeiten für einzelne Teams, Ressourcen in Microsoft 365 für Gast User unzugänglich zu machen und Gastzugriffe zu sperren. Für Bibliotheken in SharePoint, in denen geschützte Dokumente liegen, sind diese Funktionen besonders nützlich. Einzelne Dokumente können so geschützt, aber auch komplette Zugriffe auf Webseiten oder Bibliotheken gesteuert werden.

Diese spezifischen Einstellungen ergänzen ein Gast User Management-System um weitere Sicherheitsfunktionen, die parallel zum Einsatz kommen sollten.

LÖSUNGEN FÜR EIN NACHHALTIGES GAST USER MANAGEMENT

Es gibt verschiedene Tools und Lösungen, die Sie bei der Einrichtung, Verwaltung und Deaktivierung von Gastkonten unterstützen.

Gast User Management für Teams als App oder im Browser

Mit dem Gast User Manager von Arvato Systems behalten Sie die volle Kontrolle – Sie entscheiden, wer in Ihrem Unternehmen Gastbenutzer:innen einladen darf und wie der Prozess abläuft, der schlussendlich zum Gastkonto führt. Darüber hinaus können Sie Genehmigungsprozesse im Gast User Management von Arvato Systems hinterlegen und diese so einfach nachvollziehen.

Die Lösung ist als Teams App oder im Browser schnell, einfach und überall im Unternehmen abrufbar. Ein Vorteil des Gast User Managers ist die direkte Integration in Microsoft Teams, zum Beispiel über den Teams-Marketplace.

Das System erlaubt die Erstellung von Gastkonten und die Zuweisung von verantwortlichen Mitarbeitenden im Unternehmen. Das ist – wie bereits beschrieben – mit den Standardmitteln in Microsoft 365 nicht möglich. Die Verantwortlichen müssen keine IT-Spezialisten sein, um das System effektiv zu nutzen. Zuständig ist das Personal der jeweiligen Fachabteilung, die mit dem oder der Gastbenutzer:in zusammenarbeitet. Das entlastet die IT-Abteilung Ihres Unternehmens und stellt gleichzeitig sicher, dass Gastkonten unter einen fest definierten Verantwortungsbereich fallen.

Der Gast User Manager von Arvato Systems erkennt bereits vorhandene Gastkonten und kann diese nach der Implementation der Lösung automatisiert anbinden und genauso steuern, wie Konten, die über das Gast User Management

selbst erstellt wurden. Das vereinfacht die Verwaltung und stellt einen hohen Sicherheitsstandard her. Über diesen Vorgang kann das System die vorhandenen Konten mit einem Ablaufdatum versehen – inklusive einer Benachrichtigungsroutine der Gäste. So können sich diese bei Ihrem Ansprechpartner im Unternehmen melden, um das Onboarding im Nachhinein zu optimieren. Dadurch lassen sich bereits nach der Implementation einer solchen Lösung ein Großteil der vorhandenen Gastkonten auflösen, deaktivieren oder richtig zuordnen.

Microsoft 365 Managed Services und Gastkonten

Bei Microsoft 365 Managed Services handelt es sich um ein vorkonfiguriertes und damit fertiges System, das Arvato Systems Kund:innen bereitstellt. Hier lässt sich ebenfalls ein Gast User Management-System hinterlegen, um den Aufwand für den Support des Systems möglichst niedrig zu halten.

Dazu kommen die Vorteile, die sich durch den Einsatz eines Gast User Management-Systems ohnehin ergeben. Die Verantwortlichen in der Fachabteilung können Gastkonten im Self-Service erstellen und verwalten. Da Best Practices schon integriert sind, gehört Governance bereits zum Standardumfang.

Möglichkeiten mit der Software-as-a-Service-Plattform NAVOO

Innerhalb der SaaS-Plattform NAVOO für die intelligente, automatisierte Verwaltung von Inhalten sind ebenfalls Funktionen zum Überwachen und Steuern von Gastkonten und deren Berechtigungen enthalten. Besitzer:innen von Projekten können in NAVOO festlegen, in welchen Intervallen ein Audit für den Gastzugriff stattfinden soll. Dazu erhalten die Fachabteilungen Erinnerungen, die vorhandenen Gastkonten regelmäßig zu überprüfen.

FAZIT: EIN INTELLIGENTES LIFECYCLE MANAGEMENT VON GASTKONTEN IST UNVERZICHTBAR

Unternehmen treiben die digitale Transformation immer weiter voran, da IT-Lösungen alle Bereiche der täglichen Arbeit durchdringen. Dazu gehört auch die Zusammenarbeit mit externen Personen. Die Folge: Eine ständig ansteigende Anzahl an Gastkonten, die zu Effizienz- und Sicherheitsproblemen führt. Hier müssen Organisationen aller Größen gegensteuern und sicherstellen, dass Gastkonten kontrolliert zum Einsatz kommen. Nur so lassen sich Produktivität, Sicherheit und stabile Netzwerke in Einklang bringen. Das erfordert intelligente Zusatztools, die dabei helfen, den Lebenszyklus von Gastkonten zu verwalten und zu automatisieren.

Das Wichtigste zum Gast User Management im Überblick

- Mit der wachsenden Zusammenarbeit von Unternehmen mit Partner:innen, Kund:innen und Lieferunternehmen nehmen auch Datenaustausch und Videokonferenzen zu. Hier sind Gastkonten nahezu unverzichtbar, um externe Benutzer:innen anzubinden.
- Allerdings vergrößert das die Gefahr, dass Gastkonten missbraucht werden, da sie Zugriff auf Unternehmensressourcen erhalten. Denn beim Einsatz externer Benutzer:innen wird einer externen Organisation die Kontrolle über einzelne Nutzer:innen gegeben. Diese Kontrolle sollte nur an vertrauenswürdige Organisation gegeben werden, da sonst eine große Sicherheitslücke entsteht.
- Hinzu kommt eine inflationäre Verwendung dieser Konten bei gleichzeitiger unzureichender Verwaltung. Das resultiert in einer ständig wachsenden Anzahl an Konten, die vielleicht nicht mehr gebraucht, aber auch nicht gelöscht werden. Darunter leidet ebenfalls die Effizienz.
- Die Lösung ist ein effektives Gast User Management, das den Lebenszyklus von Gastkonten steuert. Diese sollten einem oder mehreren internen Verantwortlichen zugeordnet werden.
- Ein gutes Gast User Management unterstützt die Anwender:innen im Unternehmen beim Anlegen, Verwalten und Löschen von Gastkonten, ohne die Produktivität zu stören.
- Sie können die Konten überwachen und sich einen Überblick verschaffen, sodass die Verantwortlichen im Unternehmen jederzeit wissen, wie viele Gastkonten für welchen Zweck zum Einsatz kommen.
- Die Lösungen von Arvato Systems helfen dabei, Gastkonten im Self-Service anzulegen, was die IT-Abteilung deutlich entlastet. Dennoch bleiben sie jederzeit unter der Kontrolle des Systems. Regelmäßige Audits stellen sicher, dass alle vorhandenen Gastkonten tatsächlich im Einsatz sind. Bereits vorhandene Gastkonten erkennen die Systeme und binden sie mit ein.

Checkliste: Daran sollten Sie denken

- Definieren Sie den Prozess für die Anlage und Klassifizierung von Gast Usern.
- Wählen Sie ein Gast User Management, das Azure AD und Add-Ons unterstützt, wenn Sie Microsoft 365 nutzen.
- Überlegen Sie sich, wie Sie die Prozesse Ihres Gast User Managements am besten in die Verwaltung Ihrer Digital Workspace einbinden können.
- Prüfen Sie, wie sich die Verwaltung der Gast User automatisieren lässt.
- Wenn Sie einen Self-Service für die Anlage anbieten wollen, sorgen Sie dafür, dass dieser gut bedienbar und dokumentiert ist.
- Bestimmen Sie die Authentifizierung, den Schutz, MFA und Conditional Access für Gast User.
- Testen Sie das Gast User Management und die dahinterstehenden Abläufe umfassend aus Sicht der Mitarbeitenden und Gast User, um Probleme schnell zu identifizieren und zu beheben.
- Überlegen Sie sich, worauf Gäste keinen Zugriff haben dürfen, um sensible Inhalte zu schützen.
- Listen Sie aktuell vorhandene Gast User auf und überprüfen Sie diese, um sie optimal in das Gast User Management einzubinden.
- Legen Sie fest, wie der Zugriff der Gast User erfolgen soll: Sollen diese nur in der Cloud, On-Premises oder in hybriden Szenarien angebunden werden?
- Legen Sie den Ablauf von Gast Usern fest.
- Binden Sie die fachlichen Verantwortlichen dabei regelmäßig in die Überprüfung der Gastkonten ein.

- Prüfen Sie Ihre Inhalte – lassen sich bestimmte Daten von einem Zugriff durch Gastbenutzer ausschließen?
- Prüfen Sie, ob Sie den Gastzugriff für bestimmte Inhalt ausschließen können.
- Prüfen Sie nach dem Anlegen eines Gast Users, ob die Berechtigungen richtig gesetzt sind und kein Over-Sharing erfolgen kann.

Kontakt

Sie haben Fragen zum Gast User Management?

Melden Sie sich gerne bei uns!

Tim Seebrandt

Sales Consultant

Telefon: +49 5241 80 79491

E-Mail: tim.seebrandt@bertelsmann.de

www.navoo.com

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