imprivata OGITIX

RATGEBER
MICROSOFT 365 TRIFFT IAM

Alle Zugriffsrechte in hybriden Cloud-Umgebungen unter Kontrolle

Wie lassen sich die widersprechenden Philosophien der Selbstverwaltung und Kontrolle vereinigen und konkrete Lösungen realisieren?

Ein Ratgeber in Kooperation mit:

DIERICHWEILER
Unternehmens- und Prozessberatung

Inhaltsverzeichnis

1 Einleitung

In nahezu allen Unternehmen kommen inzwischen Produkte aus der Microsoft 365 Familie zum Einsatz. Wenn sie noch nicht da sind, wird zumindest über deren Einsatz nachgedacht. Der Vorteil dieser Produkte ist einfach erklärt:

Microsoft 365 bietet den Anwendern mit einer hohen Usability die Möglichkeit, ortsunabhängig zu arbeiten und zusammen zu arbeiten – von jedem unterstützten Endgerät aus. Der Zugriff auf die Daten ist immer über das Internet möglich.

Die Corona Pandemie und die damit aufkommende „Home-Office-Welle“ haben diesen Effekt noch verstärkt. Dass sich die gespeicherten Daten in Rechenzentren von Microsoft befinden, sorgt natürlich bei den Datenschützen für Kopfzerbrechen.

Aus Sicht des Identitäts- und Berechtigungsmanagements (Identity und Access Management | IAM) ergibt sich noch ein anderer Aspekt: Die Philosophie der Microsoft 365 Plattform.

2 Microsoft 365 – der mündige Nutzer

Microsoft 365 soll die Zusammenarbeit über die Grenzen von Gruppen, Abteilungen oder Organisationen hinaus sehr einfach ermöglichen. Die Standardeinstellungen der Konfiguration sollen dabei helfen, die Nutzung innerhalb und außerhalb der Organisation für den Endanwender so einfach wie möglich zu gestalten.

Ohne Anpassung der Konfiguration können Endanwender*innen neue Teamräume anlegen und gestalten, SharePoint Sites mit Ordnern und Inhalten beschicken und als Besitzer*innen deren Berechtigungen freisetzen. Ergänzend dazu können Besitzer*innen von Ressourcen beliebige externe Personen zur Zusammenarbeit einladen und Inhalte teilen.

Natürlich kann die IT vor Freigabe der Plattform diese weitreichenden Berechtigungen begrenzen und am Sicherheitsbedarf des Unternehmens ausrichten. Neben der Beschränkung der Berechtigungen sind aber alternative Einrichtungs-/Antragsmöglichkeiten zu schaffen, damit die Microsoft 365 Plattform für die gewünschte Zusammenarbeit einsetzbar bleibt.

Eine zu starke Reglementierung und damit Einschränkung der Anwenderflexibilität kann dafür sorgen, dass die Arbeitsabläufe in Microsoft 365 stark gestört werden und die Philosophie der gesamten Plattform in Frage gestellt wird.

3 Identity & Access Management – alles unter Kontrolle

Identity und Access Management Lösungen bringen geregelte Prozesse für alle Anwendungsfälle im Lebenszyklus einer Person. Alle Vorgänge sind protokolliert und nachvollziehbar, es gibt klare Regelungen für Anträge und Freigaben.

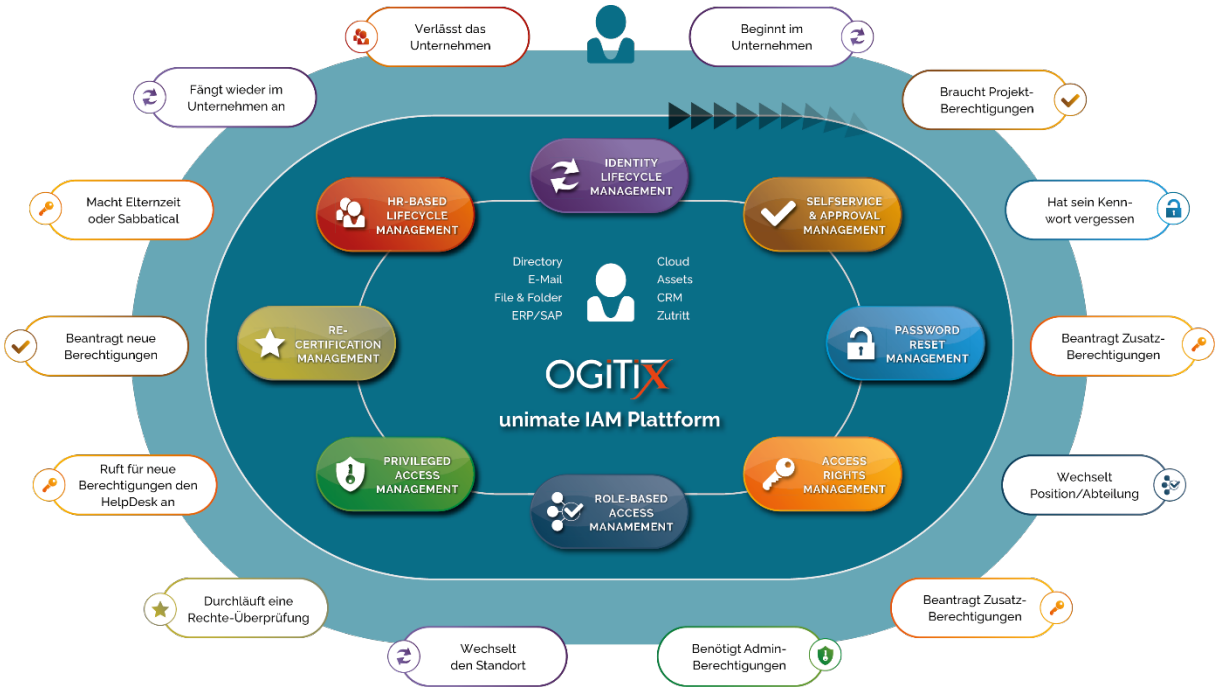


Abbildung 1: Ausschnitt aus dem Lebenszyklus einer Person im Unternehmen

Die Personen erhalten über das IAM so wenig Zugriffsrechte wie möglich und so viele wie nötig. Die IT-Sicherheit wird verbessert und Datenschutzanforderungen eingehalten. Das Identity und Access Management ist das zentrale System für die Beantragung und Vergabe von Berechtigungen.

Die Herangehensweise einer durch ein IAM-System gesteuerten IT-Umgebung zur Einrichtung neuer Personen und Ressourcen ist stark auf die Einhaltung der Compliance- und Sicherheitsregeln sowie der Überprüfbarkeit der IT-Administration ausgelegt. Dies widerspricht in vielen Punkten den Grundeinstellungen der Microsoft 365 Plattform.

4 Identity & Access Management und Microsoft 365 – Best of Both

Die eher gegensätzlichen Philosophien – einerseits Kontrolle durch Identity und Access Management und andererseits die Offenheit und Flexibilität durch die Microsoft 365 Plattform – sollten aufeinander abgestimmt werden.

Identity & Access Management	Microsoft 365
Zentrale Verwaltung aller Accounts und Berechtigungen mittels eines IAM-Systems	Der Anwender ist mündiger Nutzer und kann seine Ressourcen und Daten „teilen“
Anwender erhalten Zugänge und Zugriffe entweder rollenbezogen oder über definierte Antrags- und Genehmigungsprozesse	Integrierte Self-Services bieten Flexibilität und Agilität zum Nutzen des Unternehmens
Das IAM-System weiß jederzeit wer was, warum, durch wen genehmigt erhalten hat	Zusammenarbeit erfolgt global und meistens nach Bedarf, auch mit externen Partnern
Es erfolgt keine lokale User-Administration von IT-Systemen durch Anwender oder Admins	Grundsätzlich hat jede Ressource ihren „Besitzer“ der gleichzeitig deren Admin ist

Microsoft 365 Cloud Services sollen die Zusammenarbeit inner- & außerhalb der Organisation ermöglichen und fördern. Ein Identity und Access Management-System ist für die Einhaltung der gesetzlichen Regularien und der internen Compliance- und Sicherheitsregeln verantwortlich.

Prinzipiell ergeben sich drei mögliche Ansätze für die Integration:

1. **Microsoft 365 führt und IAM berichtet**
   Microsoft 365 führt und die Identity und Access Management-Lösung kümmert sich um die Nachvollziehbarkeit der eingerichteten Personen und Berechtigungen.

2. **IAM führt und steuert Microsoft 365 Ressourcen**
   Identity und Access Management führt und steuert Microsoft 365 analog wie andere Ressourcen (SAP, HR, AD, Zutritt u.v.m.) mit entsprechenden Prozessen.

3. **IAM steuert und erlaubt Verwaltungen in Microsoft 365**
   Identity und Access Management übernimmt die Grundadministration (Ressourcen, Gäste), bestimmte Berechtigungsvergaben erfolgen in der Microsoft 365 Plattform und werden im Identity & Access Management dargestellt und archiviert.

4.1 Microsoft 365 führt und IAM berichtet

In diesem Integrationsszenario wird die Microsoft 365 Plattform nur sehr gering eingeschränkt, d.h. Endanwender können eigene Sites/Teams nach Maßgabe und organisatorischer Vorgabe selbst erstellen und weitere Anwender einladen und berechtigen. Die einheitliche Bereitstellung der Ressourcen wie z. B. Teamräume/Sites erfolgt auf Basis von angepassten Vorlagen.

Alle Vorteile der Microsoft 365 Plattform für die fachliche Zusammenarbeit bleiben erhalten. Das Identity und Access Management-System bindet die Microsoft 365 Plattform ein – es wird aber nur „lesend" der IST-Zustand zeitpunktbezogen erfasst und im Identity und Access Management System zur Auswertung und Historisierung aufbereitet.

Das bedeutet konkret: Das Reporting im Identity und Access Management-System gibt Auskunft welche Accounts / Berechtigungen auf der Microsoft 365 Plattform eingerichtet waren. Bei Bedarf übernimmt Identity und Access Management System eine Rezertifizierung der Personen/Berechtigungen, kann das Ergebnis aber nicht in der Plattform durchsetzen, sondern informiert die jeweiligen Besitzer der Ressourcen über zu entfernende Berechtigungen.

Die Möglichkeiten zur Zusammenarbeit werden nicht durch ein Identity und Access Management System begrenzt, sondern es stehen alle Möglichkeiten von Microsoft 365 offen und das Identity und Access Management-System übernimmt passive Überwachung.

4.2 IAM führt und steuert Microsoft 365-Ressourcen

Bei diesem Integrationsansatz wird die Microsoft 365 Plattform wie alle anderen IT-Systeme über Schnittstellen an das Identity und Access Management System angeschlossen und die Administration von Benutzern, Zugriffsrechten und Ressourcen wird damit weitestgehend an das Identity und Access Management System übertragen.

Die Einrichtung von Ressourcen auf der Microsoft 365 Plattform wie Teams/Sites/Mailboxen erfolgt erst nach Antrag, Prüfung und Freigabe über die IAM-Software. Nach der initialen Bereitstellung werden auch alle Änderungen an diesen Ressourcen über das Identity und Access Management beantragt und ausgeführt. Die Anwender sind nur einfache Nutzer der Ressourcen und keine „echten" Besitzer im Sinne der Microsoft-365 Plattform, d.h. sie können die eingerichteten Strukturen nur sehr begrenzt anpassen.

Neben den Ressourcen werden auch alle externen Personen zunächst in der Identity und Access Management-Software angelegt, geprüft und freigegeben, bevor diese zur Berechtigungszuordnung und schlussendlichen Nutzung bereitstehen.

Da die Endanwender keine bzw. nur geringe Änderungsmöglichkeiten auf die Ressourcen erhalten, müssen alle wesentlichen Änderungen in der Bedienoberfläche des Identity und Access Managements verfügbar sein, so dass alle fachlichen Änderungswünsche in dieser Oberfläche angestoßen werden können. Dies umfasst z. B. die Einrichtung weiterer Nutzer, die Änderung von Zugriffsrechten sowie das Anlegen von Unterstrukturen (Kanäle, Seiten).

Die strikte Begrenzung der Änderungsmöglichkeiten auf der Microsoft 365 Plattform führt zu einer hohen Transparenz im Identity und Access Management. Die Endanwender werden es aber als nachteilig empfinden, da die Agilität der Microsoft 365 Plattform reduziert und zur Bereitstellung neuer Ressourcen, Gäste und Zugriffe die Oberfläche der IAM-Lösung genutzt wird.

Bei dieser strikten Identity und Access Management-Orientierung ist die Erfüllung aller Compliance / Security Anforderung für die Microsoft 365 Plattform allerdings gewährleistet.

4.3 IAM steuert und erlaubt Verwaltungen in Microsoft 365

Neben den beiden „extremen“ Varianten besteht die Möglichkeit, angepasste Lösungen zwischen den beiden vorgenannten Varianten zu realisieren. Allen Zwischenlösungen ist gemein, dass das Identity und Access Management die Bereitstellung der Grundstrukturen wie Ressourcen/Gast-einladung übernimmt und die Endanwender darauf aufbauend in der Microsoft 365 Plattform ergänzende Änderungen direkt vornehmen können.

Auf diese Weise können der berechtigte Wunsch und die rechtliche Anforderung zur Einhaltung der Compliance- und Security-Vorgaben auch auf der Microsoft 365 Plattform realisiert werden, ohne die „Leichtigkeit“ der einfachen Zusammenarbeit zu verhindern.

Das Identity und Access Management-System übernimmt wie bei anderen Ressourcen auch nach Antrag und Freigabe die initiale Bereitstellung der Ressource(n) sowie die Zuordnung der Berechtigungen. Die eingetragenen Besitzer nehmen weitere Anpassungen an der Ressource über die Oberfläche der Microsoft 365 Plattform vor. Das Identity und Access Management System erfasst regelmäßig den IST-Zustand der hinterlegten Berechtigungen und bereitet dies für das Reporting und die Historisierung entsprechend auf.

Das Identity und Access Management-System übernimmt den Gasteinladungsprozess, d.h. in der IAM-Software werden externe Personen erfasst und registriert sowie über definierbare Freigabeprozesse geprüft und zur Zusammenarbeit freigegeben. Im Anschluss daran legt das Identity und Access Management-System diese Personen als Kontakt auf der Microsoft 365 Plattform an, so dass die Besitzer von Ressourcen diese Personen für Ihre Ressource berechtigen können.

Auf diese Weise können Vorzüge & Aufgaben der beiden Plattformen in Einklang gebracht werden.

4.4 Empfehlung & Best-Practices

Microsoft 365-Services allein dem Anwender zu überlassen, ist riskant!

Microsoft 365 Services lassen sich weitgehend über eine IAM-Lösung verwalten

- Einladen von externen Benutzern über föderative Gast-Accounts
- Verwaltung des Lebenszyklus externer Benutzer inkl. deren Rezertifizierung
- Anlage von Microsoft 365 Gruppen und optional
  Übernahme der Besitzerrolle durch das IAM
- Verwaltung der Mitglieder in Microsoft 365 Gruppen, auch von „Gästen“
- Anlegen von neuen Microsoft Teams „Teams“ inkl. deren Microsoft 365 Gruppen

Diese Entscheidung muss jedes Unternehmen aus den eigenen Anforderungen ableiten und diese stehen in der Regel im Spannungsfeld zwischen Datenschutz, Security und Compliance einerseits und der Agilität, Flexibilität und Usability andererseits.

Unsere „Best Practice“ Empfehlungen zu Microsoft 365:

(1) **Steuern Sie den Lebenszyklus von Gästen IMMER über einen geregelten IAM-Prozess**
   - Geregeltes Verfahren, zyklische Überprüfung, klare Verantwortung
   - Kein operativer Nachteil gegenüber der Nutzung von Microsoft 365 Bordmitteln
   - Deaktivieren jeglicher „Einladung“ durch Anwender

(2) **Limitieren Sie das Recht „M365 Gruppen“ anzulegen auf eine „Sicherheitsgruppe“**
   - Keine Anlage von Teams, SharePoint, Exchange, Planner Ressourcen durch „Jedermann“
   - Beschränken Sie die Gruppe im ersten Schritt auf berechtigte Personen oder nur auf das IAM
   - Bieten Sie die Verwaltung der Mitglieder über ihre IAM-Lösung an

(3) **Überlassen Sie die Anlage von Ressourcen ggf. ihren Anwendern, aber nur auf Grundlage, von Microsoft 365 Gruppen, die Sie mittels IAM verwalten!**

Um den unterschiedlichen Ausgangssituationen und Anforderungslagen mit den verschiedensten Prioritäten sowie den unternehmensspezifischen Zielbildern gerecht zu werden, sind hierfür modulare und flexibel einsetzbare IAM-Lösungen am besten geeignet.

5 IAM-Lösungen mit OGiTiX unimate

OGiTiX unimate verfolgt mit den modularen IAM-Lösungen genau diesen Ansatz und übernimmt die punktuelle Führung, die Philosophie und Flexibilität von Microsoft 365 bleibt erhalten. Die Besonderheit besteht in den modularen Lösungen, die je nach Anwendungsfall im Kontext Microsoft 365 ein passgenaues Maß an Steuerung und Kontrolle bieten.

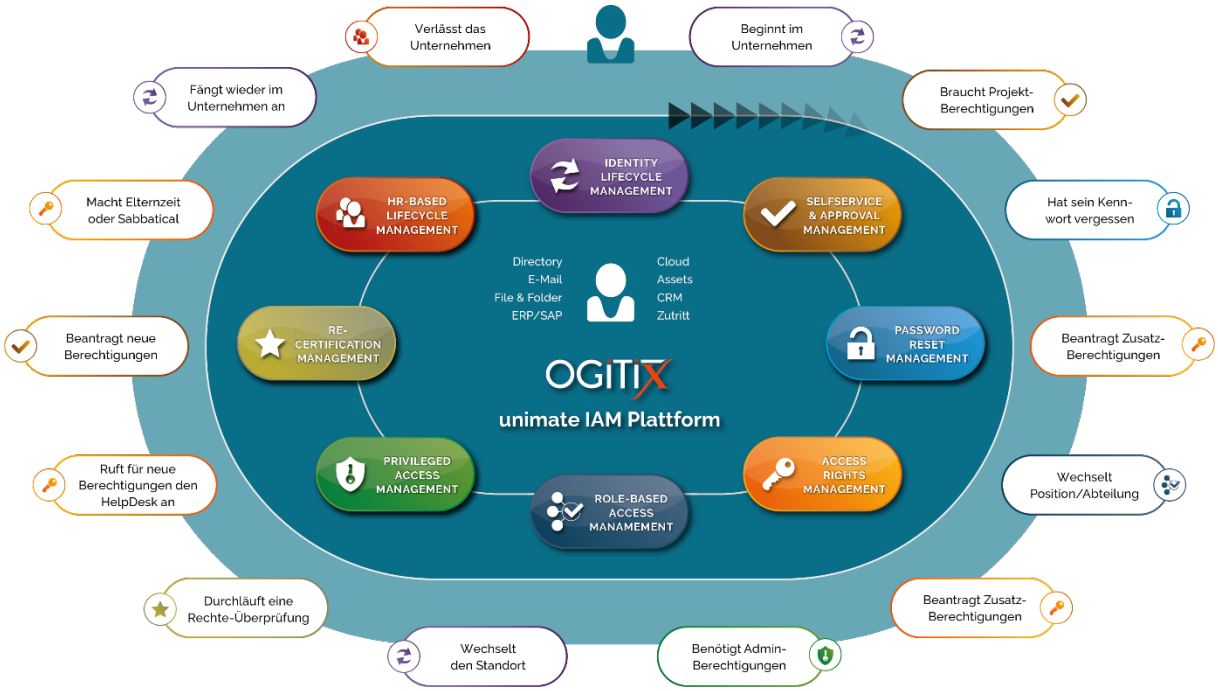


Abbildung 2: Modulare Lösungen für den Lebenszyklus von Personen

5.1 Das IAM führt mit dem unimate Identity Lifecycle Management

Mit dem unimate Identity Lifecycle Management werden die Prozesse vom Eintritt neuer Personen über verschiedene Veränderungen bis zum Austritt der Person aus dem Unternehmen gesteuert. Das unimate Lifecycle Management übernimmt dabei die digitale Prozesssteuerung für Freigaben, Prüfungen und Rechtezuweisungen. Zudem werden Benutzer, Zugriffsrechte und Ressourcen über Schnittstellen zu On-Premise-Systemen wie Active Directory oder SAP aber auch zur Microsoft 365 Cloud regelbasiert und lückenlos nachvollziehbar provisioniert.

Abbildung 3: unimate IAM-Service "Person Eintritt" (kundenspezifisch anpassbarer Service)

Bei der grundsätzlichen Integration in das Identity Lifecycle Management wird die Microsoft 365 Plattform wie alle anderen IT-Systeme über bidirektionale Schnittstellen an OGiTiX unimate angeschlossen und auch die Benutzer- & Rechteadministration weitestgehend an OGiTiX unimate übertragen. Damit ist der Grundstein für durchgängige Services gelegt.

5.1.1 Eintritt einer neuen Person

Im Zuge eines Eintritts sollte neben dem AD Benutzerkonto auch ein Azure Konto angelegt werden. Dies kann relativ einfach durch die Verwendung Azure AD Connect realisiert werden. Doch dieses neue (zusätzliche) Benutzerkonto muss mit Berechtigungen versorgt werden.

Das Lifecycle Management von OGiTiX unimate bietet hierfür eine Vielzahl von Möglichkeiten, egal ob für synchronisierte oder nicht synchronisierte Umgebungen. Die Funktionen reichen von der passgenauen Anlage der Azure Benutzerkonten und Gruppenaufnahmen, über die Verwaltung von Mailboxen und SharePoint Sites bis zur Zuweisung von Rollen und Lizenzplänen.

So entsteht nicht nur ein Benutzerkonto, sondern eine maßgeschneiderte Lösung. Benutzerkonten erhalten die richtigen Berechtigungen, werden automatisiert in die die richtigen Teams aufgenommen und sind von Anfang an arbeitsfähig. Zudem wird die Auslastung der Lizenzpläne überwacht, um auch kostenseitige Transparenz zu erhalten.

5.1.2 Veränderungen

Im Zuge des unimate Lifecycle Managements werden unterschiedliche Veränderungsszenarien verwaltet und regelbasiert gesteuert:

- Veränderung der organisatorischen Zuordnung (bspw. Abteilungswechsel)
- Stellen- oder Rollenwechsel
- Namensänderung und Änderung weiterer Personendaten
- Temporäre Abwesenheiten wie Elternzeit
- Firmen- oder Mandantenwechsel

Auch diese Änderungsszenarien haben Auswirkungen auf die Microsoft 365 Plattform. Lizenzen müssen angepasst werden, wenn sie mit organisatorischen Einheiten oder Rollen verknüpft sind. Ebenso die Mitgliedschaften und Besitzerverhältnisse in Teams oder andere Berechtigungen.

OGiTiX unimate Schnittstellen integrieren dabei Microsoft 365 Ressourcen in die verschiedenen Änderungsvorgänge und sorgen somit für Automation und Nachvollziehbarkeit:

- Azure Benutzerkonten
- Microsoft 365 Gruppen
- Microsoft Teams
- Microsoft SharePoint Online
- Microsoft Exchange Online

5.1.3 Austritt von Personen

Der Austritt ist aus Compliance-Sicht schon in „normalen" AD-Umgebungen oft eine Herausforderung. Was muss, was darf getan werden? Benutzerkennungen deaktivieren, Mail-Weiterleitungen einrichten, Abwesenheitsassistenten aktivieren, Postfacharchivierungen durchführen, Zugriffe auf das Postfach einrichten usw.

Dies ist nicht nur eine Frage der Technik, sondern auch eine Frage der Organisation und Prozessgestaltung. OGiTiX unimate bietet mit den digitalisierten Lifecycle-Prozessen und Schnittstellen unterschiedliche technische Lösungen für diese Herausforderungen.

Beispielweise kann durch die Anbindung einer HR-Software wie SAP oder Loga der Austritt erkannt und zeitgesteuert alle Konten deaktiviert werden. Weitere Arbeiten im Zuge des Austritts werden über den leicht konfigurierbaren IAM-Service geregelt.

Durch die Verwendung von Azure Benutzerkonten kommen zwei neue Dimension dazu:

1. Der Zugriff auf die Cloud-Services ist von jedem Rechner aus möglich. Das sorgt für eine höhere Anforderung an Datensicherheit und Datenschutz.

2. Die Cloud-Services sind kostenpflichtig und somit erzeugen veraltete und falsche Zugriffsrechte, Mailboxen und Konten direkte Lizenzkosten.

Zugewiesene Lizenzpläne verursachen Kosten, also muss genau darauf geachtet werden, dass die Benutzerkonten von ausgetretenen Personen stichtaggetreu keine aktiven Lizenzpläne haben.

Mitgliedschaften in Teams müssen entfernt werden. Ist die Person alleiniger Besitzer eines Teams, so muss dieses Team einer anderen Person zugewiesen werden. Auch hierfür bietet das OGiTiX unimate Identity Lifecycle Management die passenden Lösungen.

➢ **Weitere Informationen zum unimate Identity Lifecycle Management**

5.2 Punktuelle IAM-Steuerung mit dem unimate Self-Service & Approval Management

Mit dem unimate Self-Service & Approval Management werden punktuelle Antrags- und Genehmigungsvorgänge abgebildet und als 24/7-Self-Service den Anwender*innen über ein Portal bereitgestellt. So werden wichtige Compliance-, Datenschutz- oder Sicherheits-Richtlinien etabliert, eingehalten und deren Einhaltung lückenlos dokumentiert.

Abbildung 4: unimate IAM-Service "User-Self-Service" (kundenspezifisch anpassbarer Service)

So werden in der Praxis unterschiedliche Self-Services bereitgestellt, die im Kontext Microsoft 365 im Speziellen die Beantragung, Zuweisung und Verwaltung von Teams, Gästen sowie Lizenzplänen und einzelner Zugriffsrechte regeln. Aber auch Self-Services für die Beantragung von On-Premise Zugriffsrechten im AD, SAP, MS Dynamics und weiteren Applikationen können über Schnittstellen realisiert werden.

- Weitere Informationen zum unimate Self-Service & Approval Management

5.2.1 Self-Service für MS Teams (inkl. Freigaben)

Die Anlage eines Teams in MS Teams ist standardmäßig ein nicht regulierter Prozess. Das bedeutet, dass im Prinzip jeder Endanwender ein Team anlegen und konfigurieren kann. Das Ganze geschieht ohne Antrag-Freigabe-Verfahren, so dass hier ein unkontrolliertes Entstehen von Teams stattfinden kann.

Dieser aus dem Umfeld File Server und Verzeichnisse bekannte „Wildwuchs", nämlich unzählige Unterverzeichnisse, setzt man hier auf der Microsoft Collaboration Plattform fort. Mit dem entscheidenden Unterschied, dass in einem Team auch weitere Mitglieder / Gäste geladen und Dateien bereitgestellt werden können. Es hat also viel weitreichendere Konsequenzen als ein simples Verzeichnis auf einem File Server.

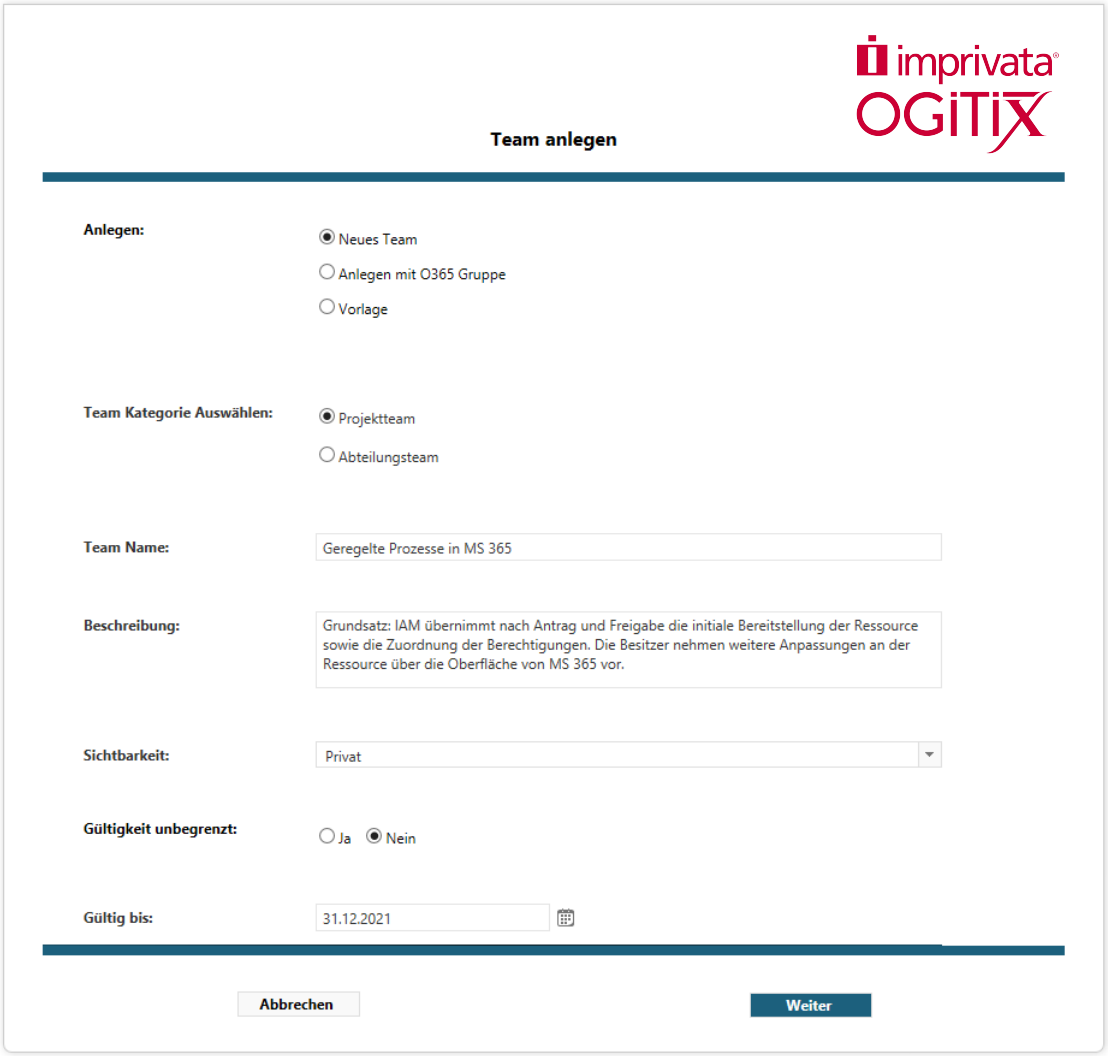
Daher liegt es nahe, das Anlegen von Teams im MS Teams Portal abzustellen und durch einen kontrollierten Self-Service, evtl. mit Antrage-Freigabe-Verfahren, zu ersetzen. Genau für diesen Anwendungsfall gibt es fertige Self-Services in OGiTiX unimate.

Die Erstellung eines Teams erfolgt in drei Schritten.

Schritt 1: Angaben zum Team

- Eingabe von Name, Beschreibung, Auswahl der Team-Art (privat, öffentlich, organisationsweit), Angabe der geplanten Laufzeit.

Der Ersteller des Teams wird automatisch auch Besitzer des Teams.

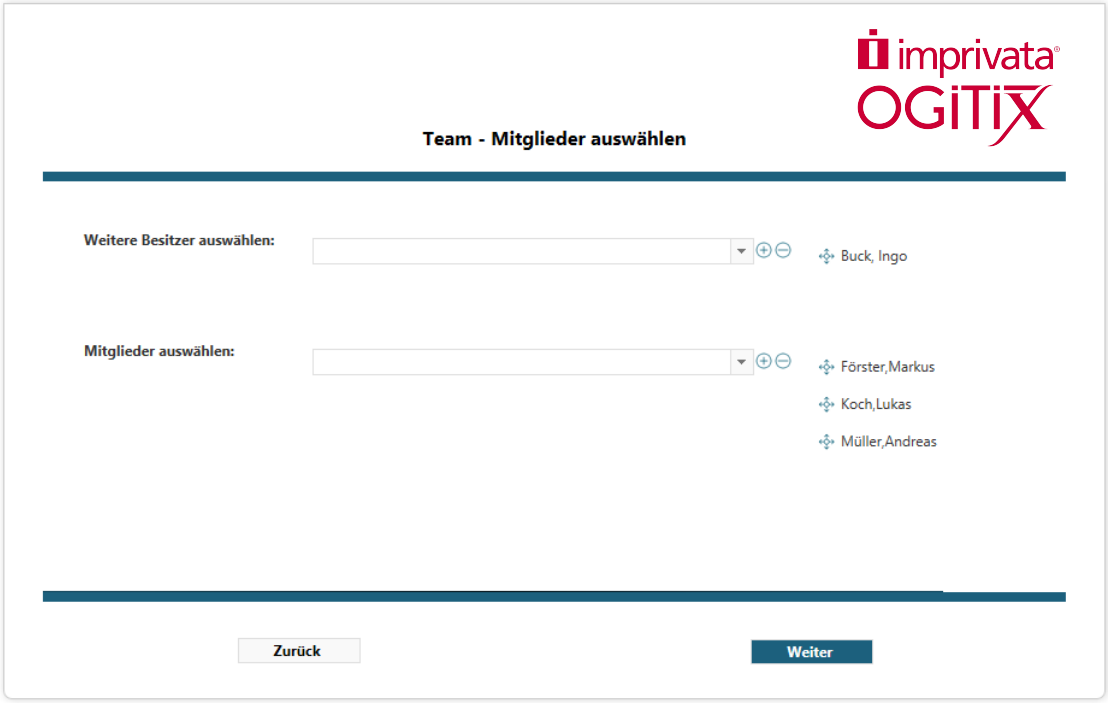


Mögliche Parametrisierungen

- Einschränkung der Team-Art (z.B. nur privat) sowie der maximalen Laufzeit.
- Vorgaben zum Aufbau des Teamnamens bzw. teil-automatische Generierung (Präfix, Suffix), z.B. aus Organisationseinheit.
- Arbeiten mit Vorlagen:
  Beim Anlegen der Teams kann aus „Vorlagen" ausgewählt werden. Diese Vorlagen sind bestehende Teams, die im unimate Datenschema durch eine zusätzliche Eigenschaft als „Vorlage" klassifiziert sind. Bei Auswahl einer Vorlage werden die Parameter dieser Vorlage, insbesondere die Kanäle, für die Anlage des neuen Teams verwendet. D.h. bei diesem Ansatz gibt es noch einen Schritt 2 (Mitgliederauswahl), aber keinen Schritt 3 (Kanäle)
- Erstellung eines Teams über die Auswahl einer bestehenden M365 Gruppe
  Bei der Erstellung eines Teams wird auch eine M365 Gruppe erzeugt. Bei diesem Ansatz dreht man die Vorgehensweise quasi um: Im ersten Schritt erfolgt die Auswahl einer M365 Gruppe, auf Basis dieser Gruppe dann die komplette Anlage des Teams. Es gibt somit keinen Schritt 2 (Mitgliederauswahl - Mitglieder kommen über die Gruppe), sondern nur noch den Schritt 3 für die Kanäle.

Schritt 2: Angaben zu Besitzern und Mitgliedern

- Hinzufügen von weiteren Besitzern:
  Auswahl von Personen, die ebenfalls Besitzer des Teams sein sollen.
- Hinzufügen von Mitgliedern:
  Auswahl von Personen, die zum Team hinzugefügt werden sollen.

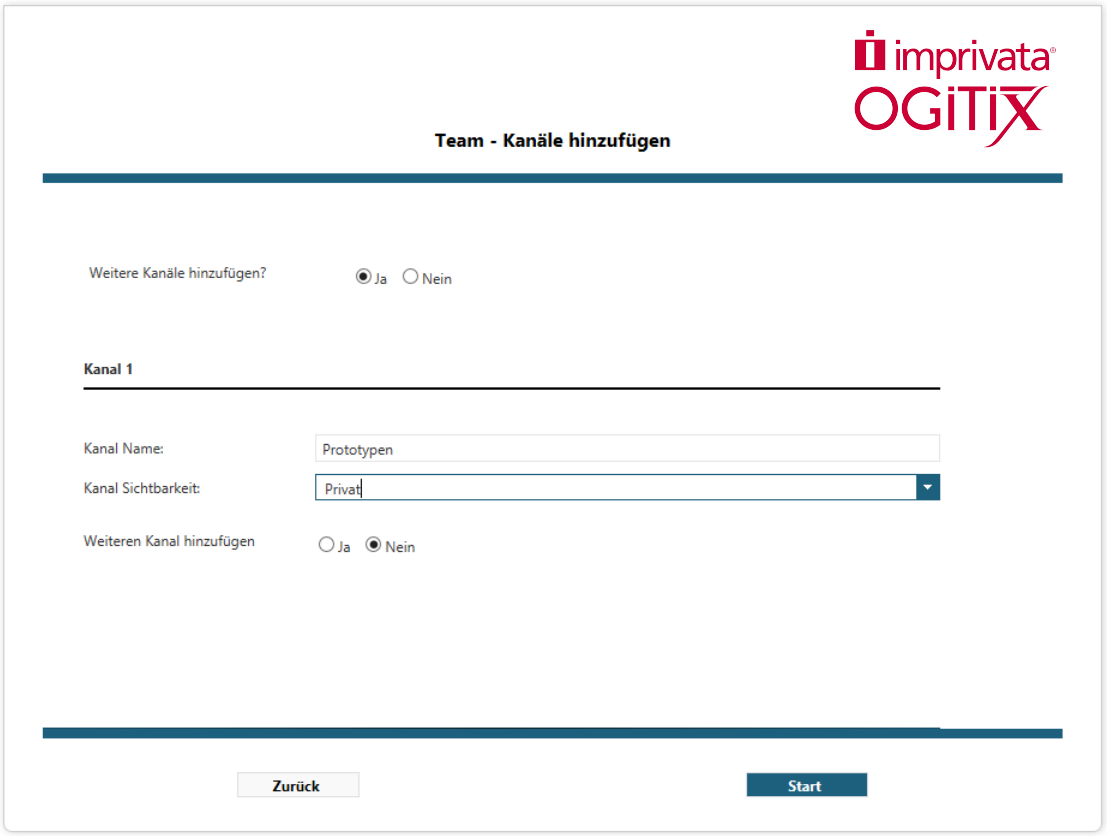


Mögliche Parametrisierung

- Einschränkung der Mitglieder, nur Identitäten oder auch Gäste?
  (Diese Einschränkung ist nach aktuellem Stand technisch nicht möglich.)

3. Angabe zu Kanälen

- Hinzufügen von Kanälen:
  Eingabe von Kanalname und Sichtbarkeit (also „Datenschutz“, Standard oder Privat)



Mögliche Parametrisierung

- Einschränkung der Sichtbarkeit: Nur Privat
  Sichtbarkeit Standard - für alle Teammitglieder zugänglich
  Sichtbarkeit Privat - nur für eine bestimmte Personengruppe im Team zugänglich

Nach Eingabe der Daten wird der Vorgang umgesetzt.

Optional kann eine Genehmigung durchlaufen werden. Dann muss die Anlage des Teams (incl. der weiteren Angaben über Mitglieder und Kanäle) durch ein oder mehrere Person(en) (Vorgesetzter, Datenverantwortliche) genehmigt werden.

5.2.2 Gast in MS Teams einladen (inkl. Freigaben)

Mit dem Gastzugriff können Personen von außerhalb der eigenen Organisation eingeladen werden, um einem Team beizutreten. Eingeladene Personen erhalten ein Gastkonto im Azure Active Directory. Diese Gastzugriffe bedingen aber ein hohes Vertrauen in deren Unternehmen.

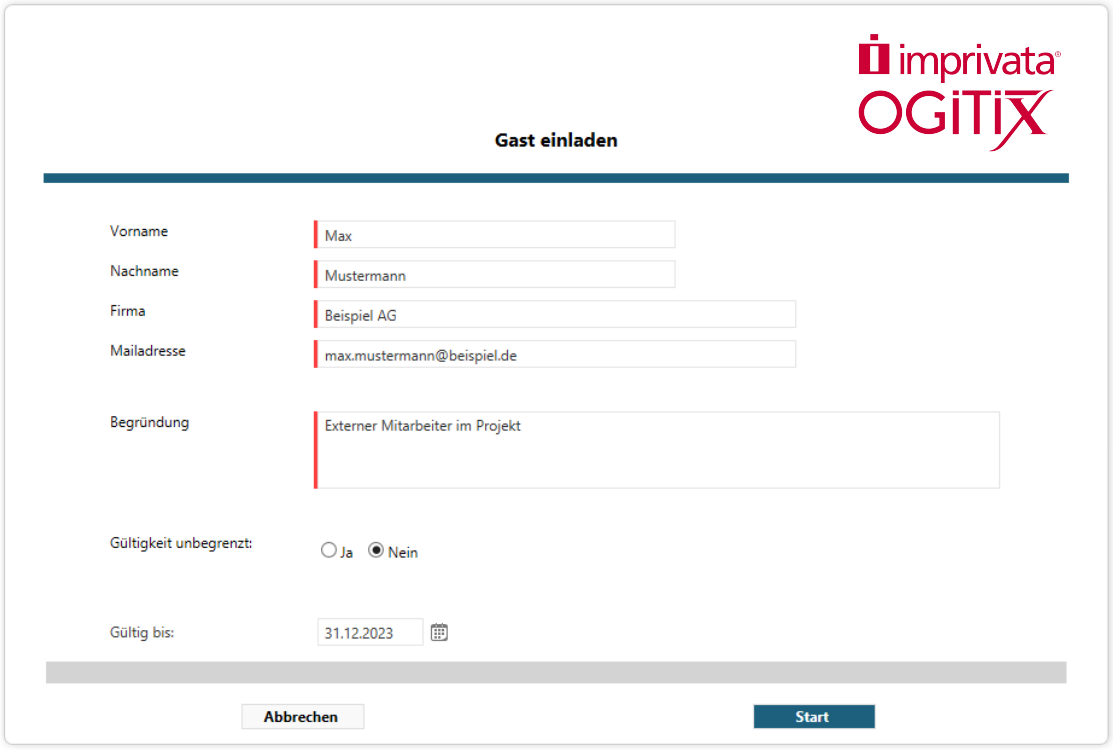
Wenn der Gastzugriff nicht reglementiert wird, kann jeder Besitzer einer Ressource Gäste einladen. Das ist wohl eines der größten Sicherheitsrisiken in der Microsoft 365 Plattform.

Daher liegt es nahe, das Einladen von Gästen im MS Teams Portal abzustellen und durch einen kontrollierten Self-Service, evtl. mit Antrage-Freigabe-Verfahren, zu ersetzen. Auch für diesen Anwendungsfall gibt es fertige Self-Services in OGiTiX unimate.

Die Einladung des Gastes erfolgt in einem Dialog.

- Eingabe von Vorname, Name, Firma, Mailadresse und Begründung.
  Außerdem erfolgt die Angabe der geplanten Laufzeit für den Gast.

Der Antragsteller wird in OGiTiX unimate zum Verantwortlichen für diesen Gast.



Nach Eingabe der Daten wird der Vorgang umgesetzt.

Optional kann eine Genehmigung durchlaufen werden. Dann muss die Einladung des Gastes durch ein oder mehrere Person(en) (Vorgesetzter, Datenverantwortliche) genehmigt werden.

Zusätzlich kann der Verantwortliche vor Ablauf des Gültigkeitsdatums eine Erinnerung erhalten, um den Gastzugang zu verlängern. Ansonsten wird der Gastzugang mit Erreichen des Gültigkeitsdatums deaktiviert.

5.2.3 Self-Services zur Verwaltung der Gastdomänen

Die Einladung von Gästen kann reguliert werden. Nicht nur dahingehend, wer Gäste einladen darf - auch die erlaubten Gastdomänen sind steuerbar.

Dazu stellt OGiTiX unimate Services bereit, mit denen die erlaubten Gastdomänen verwaltet werden können. Wird eine zuvor erlaubte Gastdomäne entfernt, wird automatisch auf Gäste aus dieser Domäne geprüft und die verantwortlichen Personen werden kontaktiert.

5.3 Reports und Analysen

Die beschriebenen Self-Services haben eine führende Rolle, d.h. die eingebauten Funktionalitäten werden in diesen Bereichen in MS Teams deaktiviert. Daneben bietet OGiTiX unimate auch verschieden Reports und Analysen, die die Rolle einer Überwachung einnehmen.

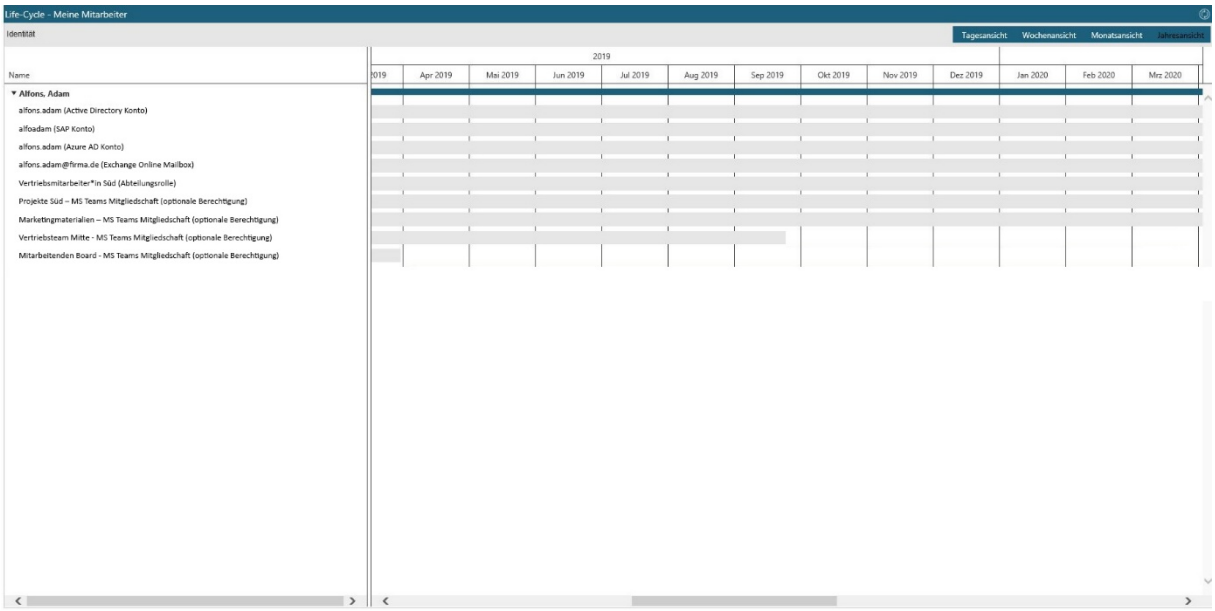


Abbildung 5: Beispiel: Lifecycle Report mit historischen Berechtigungsverlauf

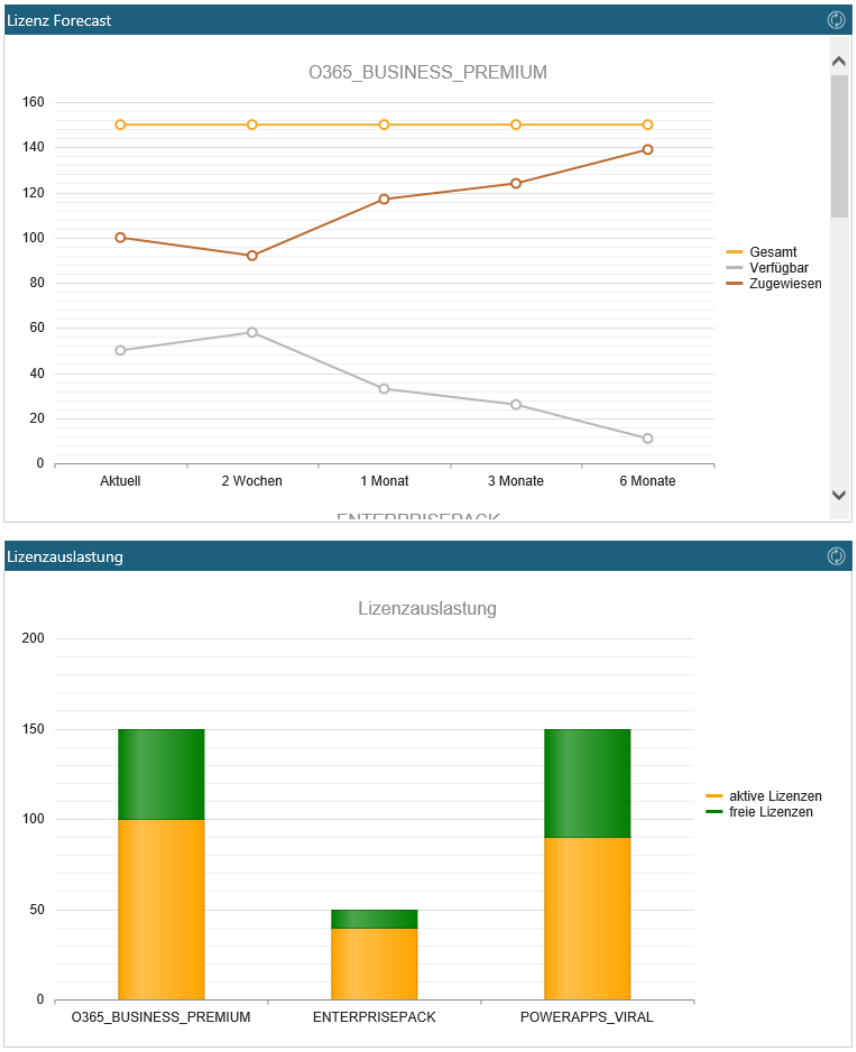


Abbildung 6: Beispiel: Lizenz-Forecast und -Auslastung

5.4 Konsolidierte Identitäts- & Berechtigungsdaten

Alle Informationen aus der Microsoft 365 Plattform werden zusammengeführt mit den Informationen aus den anderen Systemen. Damit entsteht ein Gesamtüberblick - man sieht, welche Person (Identität) in welchen Systemen (AD, Azure AD, usw.) welche Benutzerkonten und Berechtigungen hat.

Diese Information kann als Grundlage für eine systemübergreifende SoD (Segregation of Duties) Strategie verwendet werden, also die Prüfung auf das Zusammentreffen von kritischen Berechtigungen über alle Systeme hinweg.

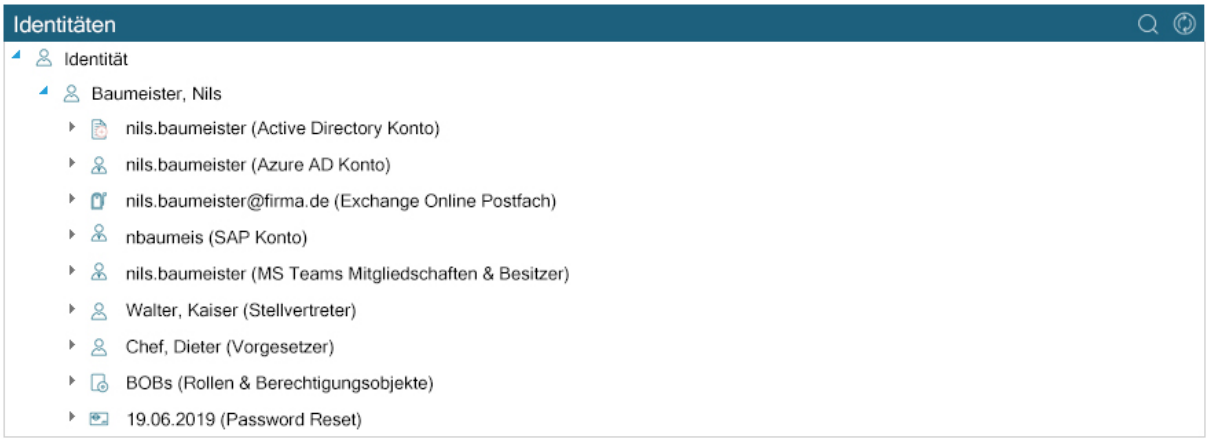


Abbildung 7: Konsolidierte Identitäts- & Berechtigungsdaten

5.5 Überwachung der Teams und Gäste

Die Teams werden in OGiTiX unimate inventarisiert und zyklisch geprüft. Teams ohne Besitzer werden gemeldet und können so neu zugeordnet werden. Teams ohne Mitglieder, also verwaiste Teams, werden ebenso gemeldet.

Außerdem erstellt OGiTiX unimate Gästelisten, d.h. Übersichten, welche Gäste Mitglied in welchem Team sind. Diese Listen können dann bei Bedarf als Grundlage für eine Rezertifizierung / Überprüfung dieser Gäste herangezogen werden.

Auch neu hinzugekommene Gäste im Vergleich zur letzten Überprüfung können auf Anforderung gemeldet werden.

5.6 IAM überwacht mit dem unimate Re-Certification Management

Für Unternehmen mit hohen Compliance-Anforderungen beispielweise aus dem Umfeld der BSI-Kritis-Verordnung, MaRisk, BAFIN oder auch ISO27001 reichen punktuelle Überwachungen und Berichte nicht aus. Dann sind zyklisch-automatisierte Überprüfungen und Bestätigungen der zugewiesenen Zugriffsrechte durch Linienvorgesetzte und Datenverantwortliche erforderlich.

Das unimate Re-Certification Management bietet diese Funktionalität: Verantwortliche überprüfen und bestätigen die Rollen und Zugriffsrechte dabei einfach im unimate Service-Portal. Die Rezertifizierung stellt so sicher, dass Personen ausschließlich über die Zugriffsrechte verfügen, die sie im Rahmen ihrer Aufgaben benötigen und diese laufend überprüft und bestätigt werden.

Abbildung 8: unimate IAM-Service "Rezertifizierung" (kundenspezifisch anpassbarer Service)

Im Zuge der Rezertifizierung werden alle Zugriffsrechte aus den angeschlossenen On-Premise- und Cloud-Applikationen eingelesen und den Daten- oder Linienverantwortlichen zur Überprüfung und Bestätigung „vorgelegt". Diese Rezertifizierung umfasst auch alle Berechtigungen und Ressourcen, auf die eine Person in Microsoft 365 Zugriff hat.

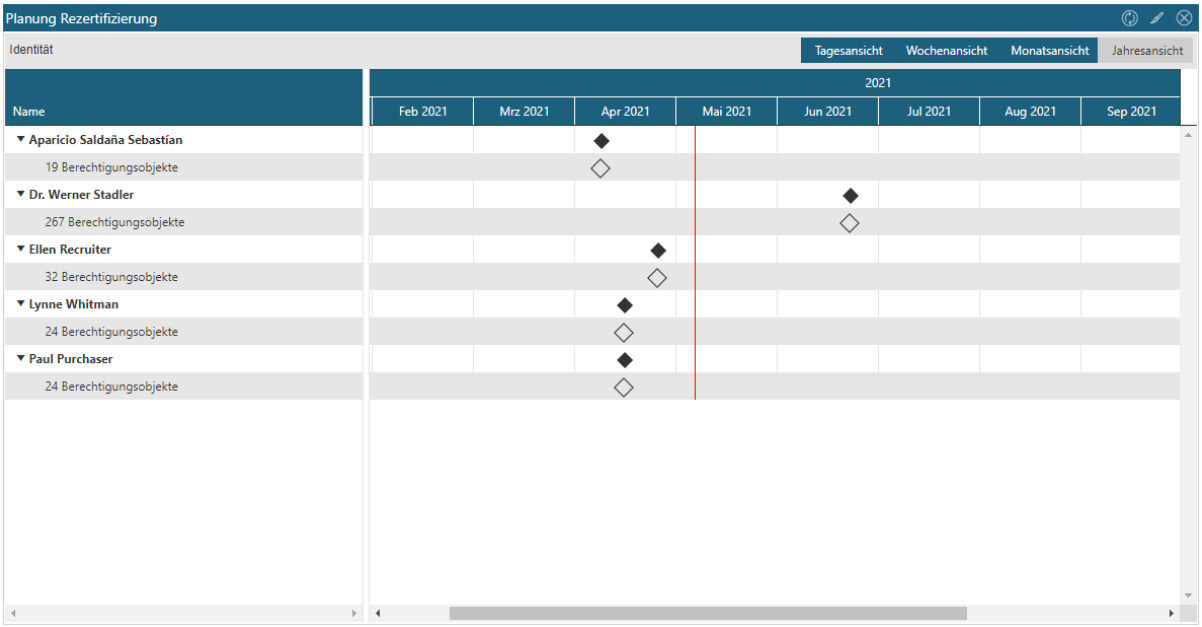


Abbildung 9: Aufgabenübersicht der aktuellen Rezertifizierung

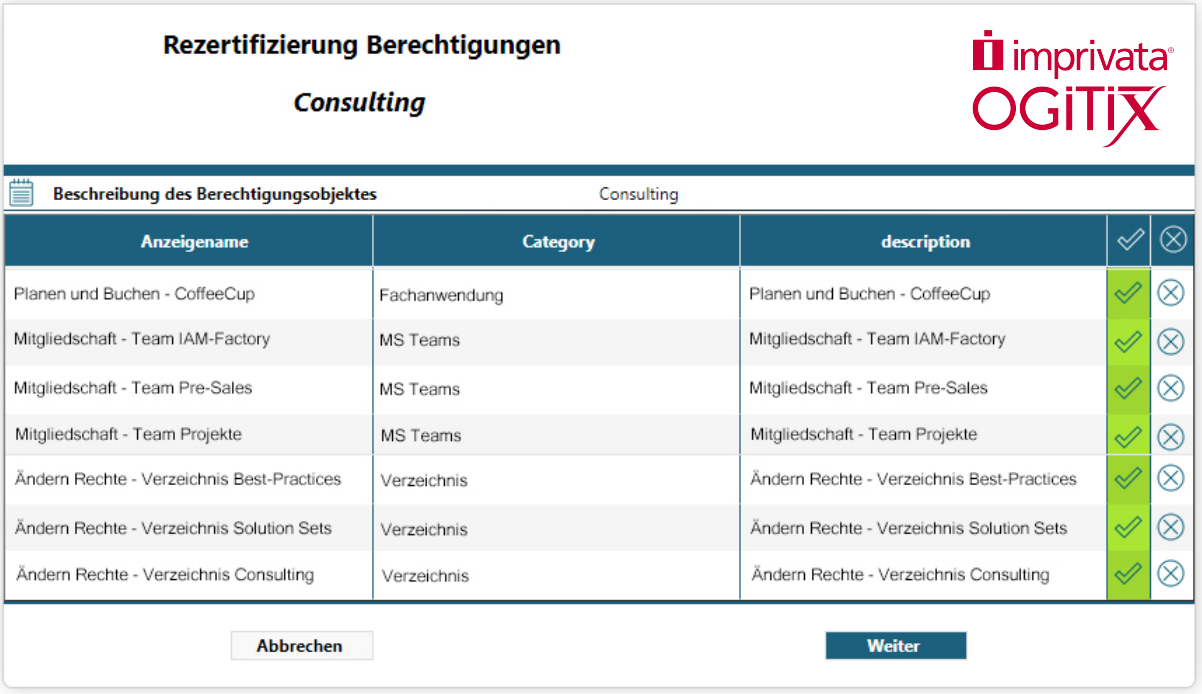


Abbildung 10: Beispiel: Aufgabe zu Rezertifizierung eines Berechtigungsobjektes

- Weitere Informationen zum unimate Re-Certification Management

6 Agiles Identity und Access Management

Digitalisierung und Automation ist die DNA von OGiTiX unimate.
Angetrieben von dem einzigartigen Unified Automation-Prinzip erlaubt die offene Plattform die passgenaue Abbildung und Automation Ihrer IAM-Prozesse, ohne coden zu müssen. Das resultiert in schnelleren Projekten sowie einem agilen Lösungsausbau und schafft strategische Mehrwerte wie Zukunftssicherheit und höhere Wirtschaftlichkeit für ihr Unternehmen.

6.1 Think Big – Start Small

Herkömmliche IAM-Lösungen geraten aufgrund komplexer und starrer Softwarestrukturen häufig in eine Komplexitätsfalle und resultieren in langwierigen Projekten. Access Rights Management-Lösungen hingegen versprechen schnelle Ergebnisse, stoßen als Insellösung aber beim weiteren Ausbau schnell an ihre Grenzen.

Unser Weg: Modulare IAM-Lösungen, die den unmittelbaren und den ganzheitlichen Lösungsansatz in sich vereinen: Think Big – Start Small!

Dieses Vorgehen ermöglicht einerseits eine direkte Problemlösung und liefert schnelle, greifbare Ergebnisse. Gleichzeitig wächst die IAM-Umgebung mit ihren Anforderungen und ist durch die offene und skalierbare unimate Plattform zukunftssicher.

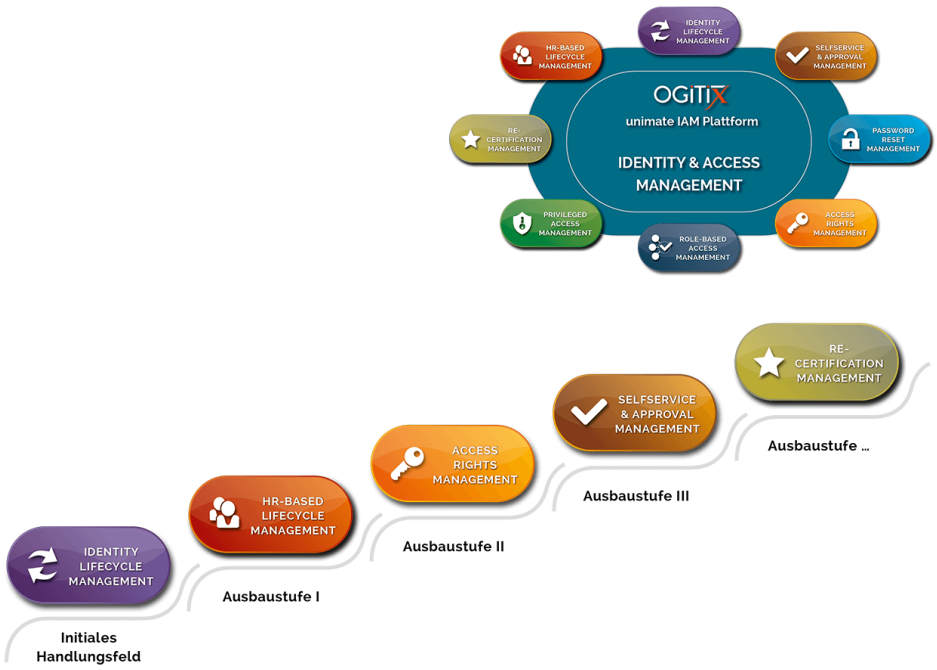


Abbildung 11: Think Big - Start Small mit modularen IAM-Lösungen

6.2 OGiTiX unimate IAM-Plattform

OGiTiX unimate steht für Unified Automation und vereint die Automatisierung operativer IT-Aufgaben mit der Automation von Geschäftsprozessen. unimate IAM-Services integrieren hierfür digitalisierte Prozesse und technische Orchestrierung und bilden so ein modulares und skalierbares Identity & Access Management.

Die Besonderheit von IAM-Lösungen auf der Basis von OGiTiX unimate besteht dabei in der intuitiven und einfachen Anpassbarkeit und Erweiterbarkeit: Alle relevanten Funktionen und Geschäftsregeln werden in einem visuellen Drag-n-Drop-Verfahren zu einem IAM-Service konfiguriert, den Sie im Handumdrehen im Service-Portal veröffentlichen.

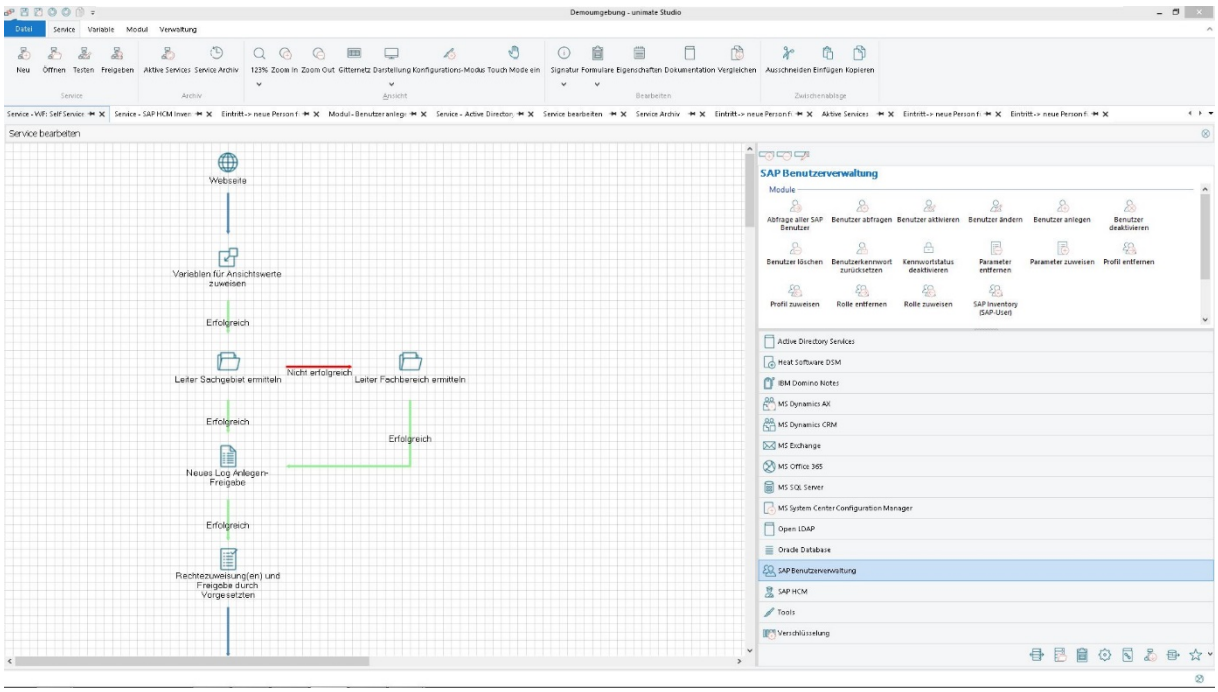


Abbildung 12: OGiTiX unimate Service-Designer

OGiTiX unimate ist als offene Plattform konzipiert und schafft die Grundlage für eine stetige Weiterentwicklung. Sie wollen neben IAM-Prozessen auch weitere Geschäftsprozesse digitalisieren oder IT-Services automatisieren? Kein Problem mit OGiTiX unimate!

Dafür bietet OGiTiX unimate alle Werkzeuge und Funktionen:

- SERVICE-PORTAL
- DIGITALE PROZESSE
- TECHNISCHE ORCHESTRIERUNG
- IDENTITY DATASTORE
- PORTAL- & FORMULAR-DESIGNER
- SERVICE- & PROZESS-DESIGNER
- SCHNITTSTELLEN-DESIGNER
- REVISIONSSICHERE PROTOKOLLE

➢ **Weitere Informationen zur IAM-Plattform OGiTiX unimate**

6.3 Exkurs: Grundlage für sichere Digitalisierung und Cloud Transition

In vielen Unternehmen sind die IT-Abteilungen derzeit damit beschäftigt, zentrale Anwendungen in die Cloud zu verlagern, um dort einen digitalen Arbeitsplatz aufzubauen. Um digitale Geschäftsprozesse schnell zu etablieren und Cloud-Services ohne große Aufräumarbeiten zu integrieren, benötigt man eine saubere Datenbasis mit korrekten Identitäts- und Organisationsdaten.

An dieser Stelle ist es hilfreich, wenn mit einer IAM-Lösung bereits alle relevanten Daten zu internen und externen Beschäftigten, Konten und Rechten an zentraler Stelle zusammengeführt wurden. Die IT-Abteilung kann sich dann im Zuge der Migration per Knopfdruck alle Identitäten anzeigen lassen und sieht sofort, wer schon umgestellt ist – ein enormer Effizienzgewinn.

Anderenfalls müsste man zunächst einmal Aufräumprozesse starten, um herauszufinden: Sind die User im Active Directory noch aktuell? Welcher der 4.000 User, die nun in der Cloud sind, sollen kostenpflichtige Services wie Office 365 erhalten? Dank der zentralen Datenbasis im IAM-System ist hier eine eindeutige Zuordnung möglich.

IAM sorgt also dafür, dass Organisationsdaten bzw. digitale Identitäten – und somit Verantwortliche und Vorgesetzte – stets aktuell gepflegt sind, ohne dass hier Risiken entstehen oder separate Tools oder Verfahren etabliert werden müssen. Dies senkt die Projektkosten für Digitalisierungs- und Cloud-Projekte. Denn es wurde eine Grundlage geschaffen, auf der digitale Geschäftsprozesse kontrolliert ablaufen. Das Unternehmen stellt so sicher, dass die richtigen Personen in Prozesse und Entscheidungen eingebunden werden.

7 Projektbericht SPIEGEL-Gruppe: Ganzheitliches IAM mit Microsoft 365

In der ersten IAM-Stufe hat die SPIEGEL-Gruppe mit OGiTiX unimate zunächst ein automatisiertes Benutzer- & Berechtigungsmanagement eingeführt. In Rahmen des Umzuges an die Ericusspitze in Hamburg wurden so die neuen Softwarelösungen für Zutrittskontrolle, Followt-me Printing und Kantinensoftware mit bereinigten und aktuellen Benutzerdaten versorgt.

In den folgenden Stufen wurden weitere Anwendungen und IT-Systeme über Schnittstellen an die IAM-Umgebung angebunden und weitere IAM-Services integriert. Neben den Standardschnittstellen von OGiTiX hat die IT-Abteilung vom Spiegel selbst für einige Systeme Schnittstellen mit dem unimate Schnittstellen-Designer generiert.

Heute läuft ein Joiner-Prozess in 30 Minuten durch", so Stephan Hardt, Leiter Digital Workplace bei der SPIEGEL-Gruppe, begeistert. Über eine neue Personalie informiert SAP HCM das BIS mit 20 Tagen Vorlauf. So bleibt genug Zeit, einen Rechner zu bestellen, die Accounts und die dahinterliegenden Workflows anzulegen, die Fachabteilung zu informieren.

Effizienter und schneller in die Cloud durch aktuelle und konsolidierte Benutzerdaten

Vor einiger Zeit hat die SPIEGEL-Gruppe den digitalen Arbeitsplatz in der Microsoft 365 Cloud realisiert. Stephan Hardt: „Die saubere Datenbasis, die wir mit OGiTiX unimate in der Vergangenheit aufgebaut haben, war uns eine enorme Hilfe, schneller und effizienter in die Cloud zu kommen. Alle relevanten Daten zu internen und externen Beschäftigten, Konten und Rechten waren bereits an zentraler Stelle zusammengeführt.

Offenes und modulares IAM bedeutet Investitionssicherheit

So ist OGiTiX unimate für den SPIEGEL-Verlag schon längst mehr als eine reine IAM-Lösung. Sie regelt nicht nur das bisherige Lifecycle-Management von Starter, Changer & Leaver – nun auch in der neuen Microsoft 365-Welt – sondern verwaltet technische Accounts, stellt Self-Services für verschiedene Abteilungen bereit und vieles mehr.

Über die Jahre ist das System mit den Anforderungen der SPIEGEL-Gruppe mitgewachsen nach dem Konzept „Think big – start small". Für Stephan Hardt ist diese Offenheit wesentlicher Grund für die Investitionssicherheit, die ihm die IAM-Lösung von OGiTiX bietet.

7.1 Download IAM-Projektbericht

Laden Sie hier den Projektbericht herunter:

- IAM Projektbericht SPIEGEL-Gruppe

7.2 Video des IAM-Projektberichtes

Sehen Sie sich hier das Video zum Projektbericht an:

- IAM Videobericht SPIEGEL-Gruppe

8 Abbildungsverzeichnis

WIR SIND IAM

SEIT ÜBER 15 JAHREN LEBEN UND ENTWICKELN WIR IAM-LÖSUNGEN FÜR SIE!

WIR ÜBERZEUGEN SIE GERNE:

MAIL TO

WEB-SEMINARE

UNSERE KUNDEN BERICHTEN:

KUNDENBERICHTE

Imprivata OGiTiX GmbH
(vormals OGiTiX Software AG)
Hans-Böckler-Str. 12
40764 Langenfeld Deutschland

Fon +49 2173 99385-0
Fax +49 2173 99385-900
Mail info@ogitix.de
Web www.ogitix.de

Vertretungsberechtigt:
Geschäftsführer Ingo Buck,
Jeffrey Kowalski

Amtsgericht Düsseldorf
Nummer: HRB 100306
Sitz der Gesellschaft:
Langenfeld