Whitepaper IAM

FLEXIBLE VERWALTUNG VON IDENTITÄTEN, BENUTZERN & RECHTEN

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INHALT

EINFÜHRUNG

IDENTITY & ACCESS MANAGER

WODURCH ZEICHNET SICH TOOLS4EVER AUS?

FAZIT

IDENTITY GOVERNANCE & ADMINSTRATION HEUTE

Die Verwaltung von Unternehmensdaten ist heute immer komplexer. Die Endanwender fordern immer mehr Flexibilität und wollen von jedem Ort mit jedem beliebigen Gerät Zugriff auf Unternehmensanwendungen und -daten haben. Das gilt sowohl für Cloud- als auch für On-Premise-Anwendungen.

Durch die gestiegene Flexibilität der Arbeitskräfte (arbeitnehmerähnliche Selbstständige, Leih- und Zeitarbeiter, Freiberufler, externe Berater) haben viel mehr Personen Zugriff auf das Unternehmensnetzwerk, als tatsächlich auf der Gehaltsliste stehen. Diese Menschen werden flexibel an verschiedenen Stellen im Unternehmen eingesetzt und auch die festangestellten Mitarbeiter nehmen in der Organisation immer stärker unterschiedliche Rollen ein, die über ihre Kernaufgaben hinausgehen.

Einerseits wird also die IT-Infrastruktur (Cloud, BYOD, Virtualisierung, Federation) komplexer. Andererseits werden die Personen, die Zugriffsrechte haben müssen, flexibler eingesetzt. Und das alles in einer Umgebung, in der die Gesetze und Vorschriften in Bezug auf die Sicherheit der Unternehmensdaten immer strenger werden (personenbezogene Daten, staatliche Verträge, Finanz- und Gesundheitsdaten). Die Behörden stellen anspruchsvollere Forderungen und konfrontieren immer mehr Organisationen mit jährlichen Audits. All dem mit manuellen Prozessen gerecht zu werden, ist eine komplexe, fast unmögliche Angelegenheit geworden.

Durch Identity Governance & Administration (IGA) ist es möglich, den strengeren Gesetzen und Verordnungen trotz einer immer komplexeren Infrastruktur zu entsprechen und dabei als Organisation weiterhin flexibel zu bleiben. Mit der Wahl der richtigen IGA-Lösung können Sie Schritt halten mit den neuesten Trends auf den Gebieten Flexibilisierung, Cloud, Virtualisierung und BYOD. Gleichzeitig fördern Sie die Handlungsfähigkeit Ihrer Organisation, denn Sie erhalten die erforderliche Technologie zur Verwaltung Ihrer Daten und implementieren gleichzeitig die Tools zur Gewährleistung der Datensicherheit und Einhaltung gesetzlicher Vorschriften. Mit einem IGA-Tool wie dem Identity & Access Manager (IAM) von Tools4ever können Sie die Identitäten und Zugriffsrechte in der komplexen Umgebung Ihres Unternehmens verwalten und kontrollieren. Ihr IGA-Konzept sollte folgende Bereiche umfassen, in denen sich IAM auf die Administration der Identitäten und Benutzer, sowie die Autorisierung der zugehörigen Rechte fokussiert.

- **Administration** behandelt die korrekte Einrichtung, Verwaltung und Deaktivierung der Identitäten und der zugehörigen Benutzerkonten entsprechend der User-Lifecycle-Prozesse.

- **Autorisierung** hat das Ziel, einem User die Rechte zuzuweisen, die er für den Zugriff auf die für seine Arbeit nötigen Anwendungen und Daten benötigt, sowie die Rechte wieder zu entziehen, sobald sie nicht mehr erforderlich sind.

- **Authentifizierung** deckt die Identifizierung des Users im Netzwerk ab und betrifft den Login-Prozess. Das kann per Benutzername und Passwort geschehen, wird aber zunehmend auch per Multi-Faktor-Authentifizierung (MFA) mit Hilfe von Zugangskarten, One-Time Passwords (OTP), Smartphone oder Fingerabdruck durchgeführt.

DEFINITION VON IDENTITY & ACCESS MANAGEMENT

Dieses Whitepaper beschreibt die Vision und die zugehörige Technologie für Identity & Access Management von Tools4ever, um Identitäten und Berechtigungen auf Ressourcen über mehrere Systeme und Plattformen hinweg konsistent zu verwalten. Innerhalb eines IAM-Systems sind aus Sicht von Tools4ever daher folgende Hauptkomponenten nötig:

1. **Identity Vault:** Um alle Identitäten verwalten zu können, muss es einen zentralen Ort geben, an dem diese gespeichert werden. Im Identity Vault können Identitäten aus mehreren Quellen gesammelt und mit den entsprechenden Benutzern in unterschiedlichen Zielsystemen verknüpft werden. Dabei können komplexe Verbindungen zwischen mehreren Identitäten und mehreren Benutzern angelegt werden. Der Identity Vault ist eine standardisierte Datenbank, die auf Tools4evers langjähriger Erfahrung mit der Verknüpfung von Quellsystemen (z.B. das HR-System) und Zielsystemen (wie ERP-, ECD/EPD- und Service-Management-Anwendungen) fußt.

2. **User Lifecycle Management (ULM):** Der Administrationsteil von IGA wird vor allem durch User-Lifecycle-Management-Prozesse bestimmt: das Anlegen, Anpassen und Deaktivieren von Benutzerkonten in verknüpften Systemen und Anwendungen. Mit einem IAM-System werden die unterschiedlichen ULM-Prozesse automatisiert, die häufig noch manuell durchgeführt werden. Die Automatisierung aller Prozesse zur Benutzerkontenverwaltung wird auch als (Auto) User Provisioning bezeichnet und durch die Verknüpfung mit mindestens einem Quell- oder Service-Management-System unterstützt.

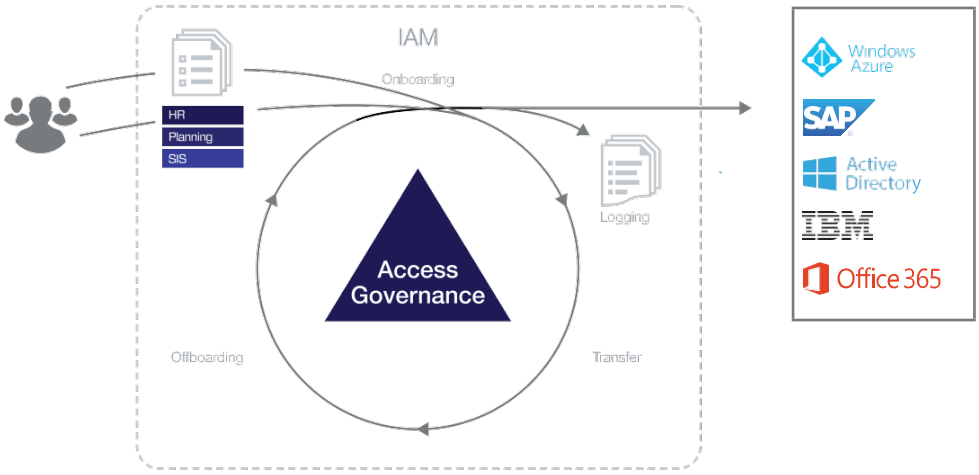
3. **Access Governance:** Das vorrangige Ziel der Autorisierungsverwaltung innerhalb eines IGA-Konzepts ist, dass Benutzer nur Zugriff auf die Anwendungen und Ressourcen haben, die für die Ausübung ihrer Funktion im Unternehmen unbedingt notwendig sind. Access Governance (AG) umfasst die Techniken und Prozesse, die dafür sorgen, dass Zugriffsrechte korrekt vergeben sind und bleiben. Schwerpunkte sind u.a. das Ausarbeiten und Verwalten des Berechtigungskonzepts, Überprüfung von Abweichungen durch verantwortliche Manager und Unterstützung bei Audits. Rollen und Rechte können sowohl automatisch als auch über ein Self-Service-Portal vergeben werden. Damit können Organisationen die ordnungsgemäße Berechtigungsvergabe äußerst flexibel gestalten.

4. **Workflow & Self-Service:** Um den Mitarbeitern die Möglichkeit zu geben, sich selbst zu helfen, und den Service Desk zu entlasten, können Benutzer und Manager Rollen und Rechte selbständig im Self-Service anfragen. Weil Antragsteller und Dateneigentümer direkt über das Self-Service-Modul interagieren, kann die gesamte technische Umsetzung der Rechteverwaltung automatisiert werden.

5. **Logging:** In diesem Bereich wird überwacht, was im IAM-System geschieht – insbesondere werden Aktionen auf den Zielsystemen protokolliert. Weil das Logging in der vorhandenen Infrastruktur oft fehlt, bietet IAM die Möglichkeit, verschiedene Aktivitäten automatisiert zu überwachen. Das sind wertvolle Informationen für Audits, um eventuelle Ausnahmen und Abweichungen von Prozessen kontrollieren zu können.

IDENTITY & ACCESS MANAGER

Ein Identity & Access Manager lässt sich schrittweise und modular in die Benutzerverwaltung integrieren und bietet die Möglichkeit alle User-Lifecycle-Management-Prozesse zu autorisieren, automatisieren und protokollieren.



ALLGEMEIN

Das Unternehmen liefert die maßgeblichen Informationen als Input für das IAM-System und entscheidet, welche IT-Ressourcen für den einzelnen Mitarbeiter nötig sind, um die Betriebsabläufe bestmöglich zu unterstützen. In Umgebungen ohne automatisiertes IAM ist häufig eine Reihe (manueller) Prozesse erforderlich, um korrekten Ressourcenzugriff für jeden Mitarbeiter zu gewährleisten. Ein IAM-System automatisiert diese Prozesse mit den wichtigsten Daten aus einem Quellsystem, meist dem HR-System. Dort ist bereits der Großteil der Informationen zum Wer, Was und Wann einer Person gespeichert.

Innerhalb einer Organisation laufen viele dynamische Prozesse ab. Jeder Mitarbeiter benötigt für seine Arbeit Zugriff auf Daten, Anwendungen, Ausstattung und vieles mehr. Welche Personen welche Arbeiten durchführen, kann sich von Tag zu Tag ändern: neue Mitarbeiter stoßen hinzu, andere verlassen das Team oder übernehmen neue Aufgaben. Auch die Organisation der Tätigkeiten ändert sich – zwar seltener, aber dafür umso deutlicher. Beispielsweise bei Umstrukturierungen von Abteilungen oder durch Änderungen von Gesetzen, Verordnungen usw.

Personen innerhalb der Organisation können unterschiedliche Positionen bekleiden, z. B. Angestellter, Lehrling, Dozent, Pfleger oder Springer. Innerhalb des IAM-Systems werden sie häufig als einzelne Identitäten angelegt, auf deren Grundlage automatisch Benutzerkonten erstellt und verwaltet werden können. Quellsysteme stellen zwar häufig alle relevanten Informationen für diese Identitäten bereit, doch nur eine IAM-Lösung ermöglicht die ordnungsgemäße Verwaltung all der komplexen Verknüpfungen zwischen Identitäten, Benutzern und Berechtigungen.

TRENDS

- **Zentrale Registrierung**
  Ein Registrierungssystem, das alle Personen erfasst, die innerhalb der Organisation tätig sind, ist die wichtigste Datenquelle für das IAM-System. Immer mehr Organisationen entscheiden sich dafür, das HR-System für die Kernregistrierung aller Mitarbeiter zu nutzen. Mit anderen Worten: Ist ein Mitarbeiter nicht im HR-System angelegt, kann er keinerlei Ausstattung vom Unternehmen erhalten, wie Schreibtisch, Laptop, Telefon, Zugangskarte oder Anmeldedaten für das Netzwerk. Mit dieser zentralen Registrierung werden alle Personen erfasst, die innerhalb der Organisation aktiv sind: Festangestellte, externe Mitarbeiter, Leiharbeitskräfte, Freiwillige usw. Dass sich diese Methode mehr und mehr durchsetzt, ist auch den strengeren Gesetzen und Verordnungen geschuldet.

- **Self-Service**
  Ein anderer interessanter Trend im Bereich IAM-Systeme: Die Anbieter von Quellsystemen integrieren immer mehr Self-Service-Komponenten, die von Organisationen immer selbstverständlicher genutzt werden. Mitarbeiter können ihre Daten im HR-System selbst einsehen und Änderungen vornehmen, beispielsweise ihre Berufsbezeichnung und Abteilung, ihr Gehalt oder verbleibende Urlaubstage. Im Ergebnis ist das HR-System somit vollständiger, aktueller, weniger fehlerhaft und damit von höherer Qualität als andere Datenquelle. Ein wichtiger Nebeneffekt: Die Verantwortung für Korrektheit und Pflege der Daten wird in die Organisation verlagert.

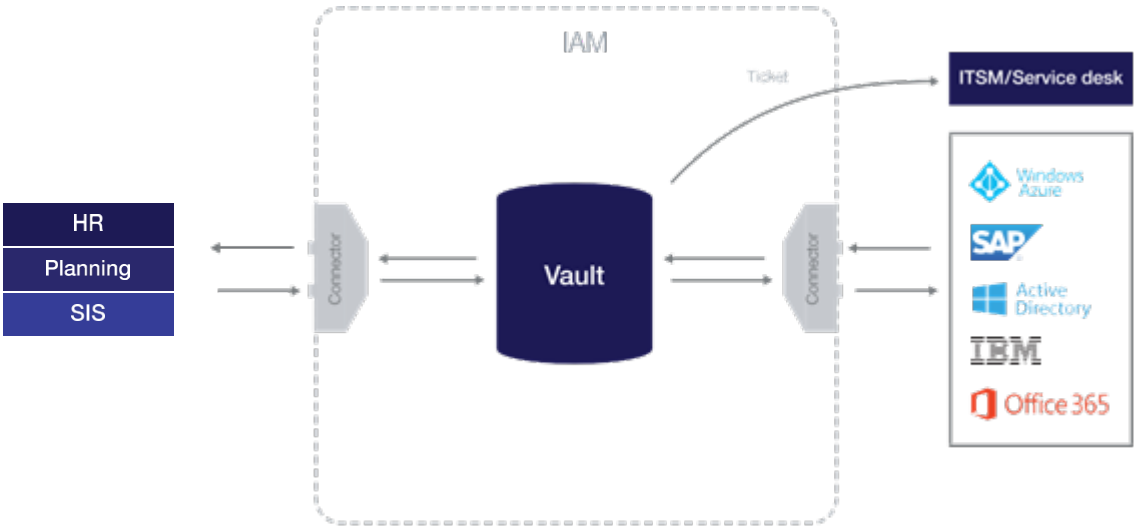
- **Reorganisation der Jobstruktur**
  Viele Organisationen haben begonnen, ihre Jobstruktur mit Hilfe von Rollen- und Funktionsprofilen zu strukturieren. Weil das HR-System eine immer zentralere Rolle einnimmt, ist es von immer größerer Bedeutung, dass eine eindeutige Jobmatrix definiert ist. Es sollte also in einer Organisation nicht fast genauso viele Funktionen wie Mitarbeiter geben, sondern stattdessen einen kleinen Satz von Funktionsprofilen und eine dazugehörige Abteilungsstruktur und Unternehmenshierarchie. Damit werden gegebenenfalls weitere Quellsysteme notwendig, um die entsprechenden Detailinformationen für das IAM-System zu liefern. Ein Beispiel dafür ist ein Dienstplansystem, wie es oft im Gesundheitssektor eingesetzt wird. Hier werden zusätzliche Informationen hinterlegt, welche Person wann an welchem Ort oder in welcher Abteilung arbeitet. Das IAM-System kann diese Information nutzen, um Rechte präziser zuzuweisen und überflüssige Rechte automatisch wieder zu entziehen.

Das Interface zwischen dem Quellsystem und dem IAM-System, der Identity Vault, ist ein zentraler Bestandteil eines Identity & Access Managers.

IDENTITY VAULT

Der Identity Vault dient als zentraler Speicher für alle Identitäten aller verknüpften Systeme. Er umfasst Identitäten, Rechte, Beziehungen und ID-Verweise zu Quell- und Zielsystemen. Der Vault ist objektorientiert, skalierbar und kann zehntausende Objekte verwalten. Gut gepflegt kann diese Datenbank dazu genutzt werden, die Synchronisierung zwischen Systemen im Bereich Identity vollständig automatisiert umzusetzen. Über Standard-Konnektoren können die Basisdaten der Identitäten aus einem Quellsystem hochgeladen werden, z.B. Ein- und Austrittsdatum, Funktion, Abteilung, Standort, Klasse, Einsatzplan etc. Je nach Branche bietet sich dafür das HR-System mit allen Mitarbeiterdaten, ein Schulinformationssystem (SIS) für Studentendaten, ein Dienstplansystem mit Daten der flexibel eingesetzten Mitarbeiter oder eine Kombination verschiedener Quellsysteme an.

Die Konnektoren sorgen für die bidirektionale Synchronisierung von Daten zwischen dem Quellsystem, dem Identity Vault und den verknüpften Zielsystemen. Tools4ever hat mehr als 200 Konnektoren entwickelt. Bei Veränderungen in den Ziel- oder Quellsystemen passt Tools4ever diese Konnektoren automatisch an. Für die meistgenutzten HR- und SIS-Systeme, on-premise und Cloud-Anwendungen, virtualisierte Anwendungen, E-Mail-Umgebungen, Datenbanken, Betriebssysteme und Verzeichnisse existieren bereits Standard-Konnektoren. Außerdem lassen sich Schnittstellen zu Service-Management-Anwendungen wie TOPdesk oder ServiceNow einrichten.



USER LIFECYCLE MANAGEMENT

User Lifecycle Management (ULM) bzw. Identity Lifecycle Management (ILM) bezeichnet die (automatisierte) Verwaltung der digitalen Identitäten in einer Organisation über ihren gesamten Lebenszyklus. Das umfasst das Anlegen, Anpassen und Entfernen von Benutzern in der IT-Infrastruktur und den Zielsystemen. Gesteuert wird das ULM über eine Reihe von Standard-Triggern und -Prozessen, die im IAM-System konfiguriert werden können. Diese Prozesse sorgen für den korrekten, technischen Ablauf von Onboarding, Stellenwechsel sowie Offboarding. Dafür werden für jede verknüpfte Anwendung Felder und Werte definiert, die für den organisatorischen Bedarf relevant sind, z.B. Einstellungs- oder Kündigungsdatum, bevorzugte Namenskonventionen oder Organisationsdaten wie Funktion, Abteilung, zuständiger Manager, Telefonnummer etc.

Die ULM-Prozesse stellen die Grundlage für erfolgreiches Identity & Access Management dar und legen fest, für wen und wann ein Benutzerkonto angelegt, geändert oder deaktiviert wird. In einem IAM-System können diese Benutzerverwaltungsprozesse auf Basis individueller Kunden-anforderungen eingerichtet und automatisiert werden. Üblich ist beispielsweise, das Benutzer-konto und die Mailbox eines neuen Mitarbeiters schon vor dem ersten Arbeitstag anzulegen. So können neue Arbeitnehmer bereits vor ihrem tatsächlichen Arbeitsbeginn E-Mails oder Tickets erhalten und in Terminplanungen einbezogen werden.

Unterstützung des Service Desk

Ein weiterer wichtiger Zweck eines IAM-Systems ist die Unterstützung des Service Desks, um alle Aufgaben, die nicht automatisiert werden können, trotzdem kontrolliert zu verwalten. Über das IAM-Portal können spezifische Aufgaben des Service Desks, wie die Vergabe von Rechten oder die Verwaltung von Benutzerkonten, einheitlich und nachprüfbar durchgeführt werden, ohne dass weitreichende Rechte in der IT-Infrastruktur für die Service-Mitarbeiter nötig sind. Dies hilft, die Administratorenrechte in der aktuellen Infrastruktur zu reduzieren.

ACCESS GOVERNANCE

Vereinheitlichung

Access Governance (AG) ist ein wichtiger Bereich innerhalb von IAM. AG muss sicherstellen, dass Mitarbeiter auf die Netzwerkressourcen Zugriff haben, die sie für ihre Arbeit benötigen, jedoch keine unbefugten Zugriffsmöglichkeiten bestehen. Durch die Verschärfung von Gesetzen und Verordnungen (DSGVO, ISO 2700x), die zunehmende Automatisierung von Arbeitsprozessen und die immer komplexere IT-Infrastruktur (Cloud, Virtualisierung, Outsourcing, gemeinsame Rechenzentren) ist AG in den letzten Jahren immer bedeutsamer geworden. Ursprünglich war Access Governance nur für Finanzinstitutionen und große internationale Unternehmen relevant. Immer stärker findet sie aber auch Anwendung im Gesundheitswesen, in mittelständischen Unternehmen (300 bis 5000 Mitarbeiter) und anderen kommerziellen Organisationen.

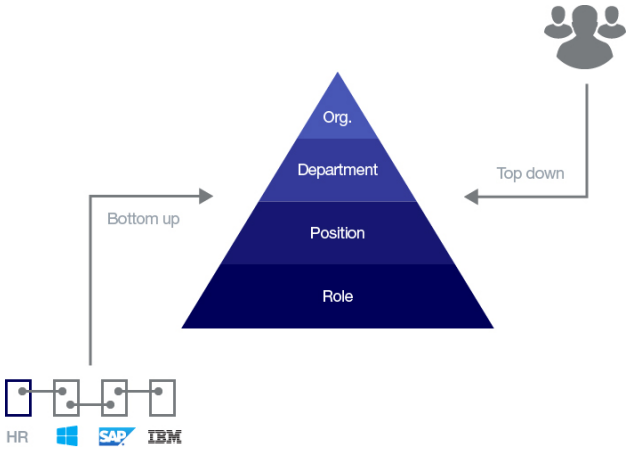
Access Governance vereinfacht die verschiedenen Formen der Sammlung und Festlegung von Rechteinformationen. Ein IAM-System bietet eine einheitliche Speichermethode, bei der die Identitäten und zugehörigen Berechtigungen miteinander korreliert werden. In vielen Organisationen liegt hier ein Engpass vor, da diese Art von Informationen meist in mehreren Systemen, unterschiedlichen IDs und verschiedenen Formaten gespeichert sind. Für die Harmonisierung und Analyse ist allerdings eine eindeutige ID pro Identität nötig.

Der Verwaltungsrat, der Vorstand und daher auch die Sicherheitsbeauftragten wollen und müssen kontrollieren, wer wo Zugriff hat. Sich manuell einen Überblick über die Rechtestruktur innerhalb der Organisation zu verschaffen bzw. diese manuell zu verwalten, ist eine enorm komplexe und zeitraubende Aufgabe. Viele Organisationen stecken jedoch bei der Verwaltung von Rechten noch in den Kinderschuhen. Es fehlen Kenntnisse der richtigen Vorgehensweise und die nötige Software. Berechtigungen werden aktuell auf Basis von Beispielnutzern zugeteilt (Copy User: „Johanna wird die gleichen Arbeiten durchführen wie Martin.“), nach Vorlage (Template User auf Organisations- oder Abteilungslevel), mit Hilfe von Tabellen oder kleinen, selbst entwickelten Anwendungen. Mit diesen Methoden wird die Zuweisung von Rechten noch ansatzweise korrekt gehandhabt. Der Entzug von Rechten ist dagegen oft nicht geregelt.

Ein IAM-System bietet die Möglichkeit, die Rechtestruktur phasenweise aufzubauen. Access Governance holt Organisationen auf der Erfahrungsstufe ab, auf der sie stehen, und führt sie schrittweise zu einer professionellen Plattform, mit der alle Berechtigungen kontrolliert verwaltet werden können.

Bestandsaufnahme der aktuellen Berechtigungen

Der erste Schritt zur Einführung von Access Governance ist eine Bestandsaufnahme, wie die Rechte aktuell im Netzwerk vergeben sind und welche Informationen darüber in der Organisation bekannt sind. Der aktuelle Status kann auf zwei Arten bestimmt werden:



- Der **Top-Down-Ansatz** inventarisiert die Berechtigungsstruktur mithilfe von Informationen, die Service Desk, Geschäftsleitung und Sicherheitsbeauftragten vorliegen. Es gibt eine Reihe von Grundrechten (*birthrights*), die jeder Mitarbeiter seine Arbeit benötigt. Beispiele dieser bekannten Rechte sind abteilungsinterne Ordner und E-Mail-Verteiler oder Gruppenmitgliedschaften, die jeder Mitarbeiter erhält (z.B. für Citrix oder Intranet). Für die wichtigsten oder kritischsten Rechte gibt es mitunter bereits eine (teilweise) Bestandsaufnahme, weil in Unternehmensrichtlinien oder durch Gesetzesvorschriften festgelegt ist, wem sie zuerkannt werden dürfen. Daher wird diese Methode wird oft als *Top-Down* bezeichnet.

- Beim **Bottom-Up-Ansatz** werden Informationen aus dem HR-System (Jobstruktur und Funktion der Mitarbeiter in der Organisation) und die tatsächlich vergebenen Berechtigungen in den jeweiligen Systemen (Active Directory, Exchange, SharePoint, ERP, Datastorage / Shares) gesammelt und zusammengeführt. Diese Methode wird auch als *Role Mining* bezeichnet – die Rollen werden faktisch aus der aktuellen Netzwerksituation abgeleitet. Dabei muss jedoch für jede Rolle eine separate Analyse vorgenommen werden, um sicherzustellen, dass die Rollenberechtigungen korrekt sind.

Eine Kombination aus *Top-Down-* und *Bottom-Up*-Prinzipien hat sich bei der phasenstrukturierten Implementierung von IAM bewährt. Zunächst konzentriert sich die Access Governance auf die meistgenutzten Rechte. So sollen Service Desk und IT-Administratoren sofort entlastet, sowie der Zugriff auf kritische Anwendungen und Daten gesichert werden. Diese Basisrechte können zügig eingeführt und per IAM-System verwaltet werden.

Für eine umfangreiche Bestandsaufnahme und Analyse aller aktuellen Berechtigungen ist eine Simulationssoftware essentiell, mit der innerhalb eines bestimmten Zeitraumes die tatsächliche Nutzung der Zugriffsrechte im Dateisystem erfasst werden kann. Auf Basis der Analyse kann ein umfangreiches, bereinigtes Berechtigungskonzept erstellt und mit dem IAM-System umgesetzt werden.

Rollenentwurf

Im zweiten Schritt werden die gesammelten Rechteinformationen aus Schritt 1 in ein Rollenmodell übertragen. Durch die Übersetzung von Systemrechten in Business-Rollen wird es für Manager viel einfacher, die Rechte zu beurteilen und sie Mitarbeitern zuzuweisen. Es gibt eine Vielzahl gängiger Rollentypen innerhalb von Access Governance, sodass das Rollenmodell modular aufgebaut werden kann. Dieser Schritt ist äußerst wichtig und bildet das Fundament eines erfolgreichen Access-Governance-Konzepts.

Die festzusetzenden Rollen müssen unabhängig von Abteilung, Funktion oder Standort bestehen, damit Veränderungen in der Organisationsstruktur nur begrenzt Auswirkungen auf das Rollenmodell haben. So wird verhindert, dass die Zeit, die in den Entwurf des Rollenkonzepts gesteckt wurde, bei jeder Veränderung in der Organisation wiederum investiert werden muss. Das gleiche gilt für die Verknüpfung der entsprechenden Rechte in den IT-Systemen. Ein solide aufgebautes Rollenmodell kann hier die Auswirkungen bei Änderungen der IT-Infrastruktur minimieren und sogar dazu genutzt werden, den Rollout von neuer Software zu vereinfachen.

Aktivierung des Rollenkonzepts

Im letzten Schritt wird das entwickelte Rollenmodell im IAM-System umgesetzt und auf neue Mitarbeiter angewendet, während sie verschiedene Stationen in der Organisation durchlaufen. Die Rollen und die zugeordneten Berechtigungen (*entitlements*) werden auf die angebundenen Zielsysteme angewendet.

Operative Veränderungen werden über das Rollenmodell im IAM-System auf drei Arten verarbeitet:

1. **Änderungen im Quellsystem**
   Wenn ein neuer Benutzer im Quellsystem hinzugefügt wird, muss festgelegt werden, welche Funktion und Rolle dieser Mitarbeiter in der Organisation einnimmt. Bei Namensänderungen, Beförderungen sowie Abteilungs-, Klassen- oder Standortwechseln in der Datenquelle erfasst das IAM-System die geänderten Attribute und vergibt anhand des Rollenmodells die entsprechenden Berechtigungen. Gleichzeitig werden nicht mehr legitime Rechte automatisch entzogen, um Rechteanhäufung zu verhindern.

2. **Regelmäßiger Verifizierungsprozess**
   In regelmäßigen Abständen prüft ein geplanter IAM-Prozess, ob im Rollenmodell, im Identity Vault oder den Zielsystemen Änderungen der festgelegten Attribute vorgenommen wurden. Dieser Prozess weist allen Benutzern entsprechend des aktuellen Rollenmodells erneut die richtigen Berechtigungen zu und entzieht gegebenenfalls veraltete, unnötige Rechte. So wird gewährleistet, dass das Rollenmodell immer maßgebend ist und Änderungen auf alle User angewendet werden.

3. **Self-Service-Shop**
   Auf Basis des Rollenmodells können über einen Self-Service-Shop auch zusätzliche Rollen durch den Mitarbeiter oder dessen Vorgesetzten beantragt werden. Sobald die Anfrage im entsprechenden Workflow bewilligt wurde, werden die zusätzlichen Berechtigungen direkt vom IAM-System zugeteilt. Damit haben Organisationen auch die Möglichkeit, die Zuteilung und den Entzug von Rechten in die Hände der jeweils verantwortlichen Person zu legen. Zum einen wird so eine inkorrekte Rechtevergabe durch den Service Desk verhindert. Zum anderen erhält das Führungspersonal zusätzlich die Möglichkeit, eine Rolle jederzeit wieder zu entziehen und die Berechtigungsstruktur so sauber wie möglich zu halten.

Die phasenstrukturierte Implementierung eines IAM-Systems bietet die Möglichkeit, einen Teil des Rollenkonzepts sofort zu aktivieren, um direkt Mehrwert zu schaffen. Standardmäßig werden nur die im Rollenmodell festgelegten Berechtigungen zugeteilt und auch nur die Berechtigungen, die im Rahmen des Modells vergeben wurden, wieder entzogen. So kann das Rollenmodell direkt eingesetzt werden, ohne dass im Vorhinein eine vollständige Bestandsaufnahme aller Berechtigungen durchgeführt werden muss. Die Wertschöpfung beginnt bereits am ersten Tag.

WORKFLOW & SELF-SERVICE

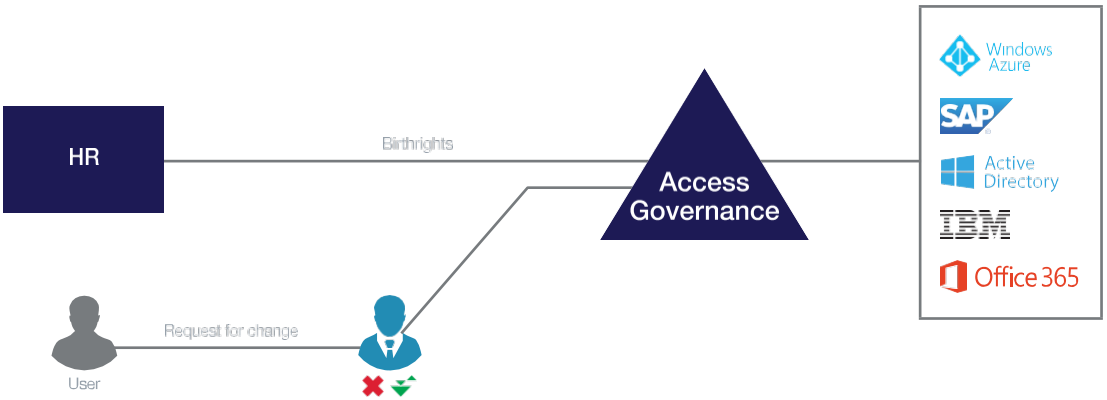
Mit Workflow- und Self-Service-Komponenten können Mitarbeiter über ein Web-Interface einfach und selbständig Rollen oder Rechte beantragen bzw. entziehen. Das IAM-System führt die entsprechenden Änderungen in der IT-Infrastruktur automatisch aus. Dieses Verfahren knüpft an den aktuellen Trend zum Self-Service an, um Mitarbeitern und Managern via IAM-System zu ermöglichen, sich innerhalb fester Rahmenbedingungen selbst zu helfen.

Ein weiterer Trend, der Self-Service-Möglichkeiten für Organisationen so wertvoll macht, ist die Reduzierung der Funktionsprofile innerhalb der Jobstruktur. In der Regel reichen die *Birthrights* aus dem HR-System für einen neuen Mitarbeiter aus, um die erste Zeit arbeiten zu können. Meist bekommen Mitarbeiter allerdings von ihren Managern regelmäßig zusätzliche Aufgaben, für die zusätzliche Netzwerkressourcen (Zugriff auf Anwendungen, Daten, Shares) benötigt werden. Auch hier gibt das Self-Service- und Workflow-Management den Mitarbeitern die Möglichkeit, selbst Anfragen nach den nötigen Rechten zu stellen – innerhalb der Grenzen des definierten Rollenkonzepts im AG-Modell.

Standardmäßig sehen die ULM-Prozesse im IAM-System vor, dass der Manager des neuen Mitarbeiters bereits vor dem ersten Arbeitstag zusätzliche Rechte zuweisen kann. Beim Onboarding müssen viele Dinge mit verschiedenen Verantwortlichen abgesprochen und geregelt werden, um den Zugriff auf (Cloud-)Anwendungen, Systeme, Daten und E-Mails zu ermöglichen. Dies kann ein langwieriger Prozess sein, wenn erst am ersten Arbeitstag damit begonnen werden kann. Wird die Prozedur aber bereits im Vorhinein und mit einem Genehmigungs-Workflow durchgeführt, kann der neue Mitarbeiter bereits am ersten Tag produktiv arbeiten. Dabei nimmt der Manager eine zentrale Rolle ein. Er kann für seinen Mitarbeiter Rechte beantragen bzw. genehmigen. Je nach Art der Anfrage sind weitere Verantwortliche wie Lizenzmanager, Sicherheitsbeauftragte, Facility- oder IT-Mitarbeiter (in der Rolle des Dateneigentümers) in den Genehmigungsprozess einbezogen. Nachdem alle nötigen Bewilligungen erteilt wurden, werden Berechtigungen über das IAM-System automatisiert in der IT-Infrastruktur zugewiesen, noch bevor der Mitarbeiter seinen Dienst aufnimmt. Auch hier findet sich der Rückbezug auf den Markt-Trend zum Self-Service wieder, der gleichzeitig den Service Desk von der manuellen Bearbeitung zusätzlicher Rechteanfragen entlastet.

Zuletzt ermöglicht ein Workflow-Modul außerdem die Dokumentation der Berechtigungsverwaltung. Dank des sogenannten Audit Trails ist mit einem IAM-System immer nachvollziehbar, wer wann ein Zugriffsrecht für einen bestimmten Mitarbeiter bewilligt hat.

LOGGING



Die Erfassung von durchgeführten Aktionen ist ein wichtiger Bestandteil jedes IAM-Systems. Im Audit Log wird festgehalten, welche Änderungen über das IAM-System durchgeführt wurden und wer welche Elemente außerhalb der grundlegenden IAM-Prozesse verändert hat, sodass alle Aktionen zurückverfolgt werden können.

Interne und externe Auditoren können anhand dieses Audit Logs jederzeit nachvollziehen, wer wann welche Aktionen durchgeführt hat – in den meisten Directories ist das nicht möglich. Manuelle Änderungen können so besser kontrolliert werden. Alle ausgeführten Aktionen lassen sich individuell pro User darstellen, beispielsweise die Aktivierung oder Deaktivierung eines Benutzerkontos, die Zuteilung weiterer Berechtigungen oder Gruppenmitgliedschaften oder ein Passwort-Reset im Active Directory. So unterstützt Logging innerhalb eines IAM-Systems die Einhaltung der strengeren Gesetze und Verordnungen in Bezug auf die Sicherheit von Unternehmensdaten.

WODURCH ZEICHNET SICH TOOLS4EVER AUS?

Tools4ever bietet Unternehmen eine einzigartige und innovative Enterprise IAM-Lösung mit einem effektiven, phasenbasierten Implementierungsansatz, der schnell zu Resultaten führt. Tools4evers Identity & Access Manager sorgt dafür, dass Organisationen auf strukturierte Weise die Kontrolle über die Verwaltung von Identitäten und Rechten erlangen.

Der IAM-Markt wird immer reifer und alle Marktbeteiligten sind sich einig, welche Funktionalitäten IAM-Systeme bieten müssen. Viele Zulieferer bieten Lösungen an, die grundsätzlich passend wirken, aber in der Implementierungsphase aufgrund von schlechter Planung oder fehlenden Modulen zu Überraschungen oder viel zusätzlichem Aufwand führen. So bringen IAM-Implementierungen häufig – statt der gewünschten Kontrolle und Sicherheit – nur große Enttäuschungen: Der interne Arbeitsaufwand und die Implementierungszeit werden deutlich überschritten und die Resultate bleiben aus.

Im Folgenden stellen wir Ihnen detailliert die Elemente vor, die den Identity & Access Manager (IAM) von Tools4ever auszeichnen, um Sie bei der Verwaltung von Identitäten und Rechten optimal zu unterstützen. IAM spart für Sie Zeit und Geld mit der Automatisierung Ihres User Lifecycle Managements, unterstützt Datensicherheit durch die Bereinigung und Reduzierung Ihrer Berechtigungsstruktur mit Hilfe eines Access-Governance-Modells und sorgt für Compliance durch umfassende Dokumentation der Benutzerverwaltungsprozesse.

IMPLEMENTIERUNG IN PHASEN

Bei der Implementierung einer IAM-Lösung durchläuft eine Organisation verschiedene Reifephasen der Professionalisierung ihres Identity & Access Managements. Dabei liegt der Fokus sicherlich nicht allein auf der IT, sondern zunehmend ganzheitlich auf allen Unternehmensprozessen der Benutzerverwaltung (Provisioning, Workflow Management, Access Governance und Self-Service). Um die IAM-Implementierung überschaubar zu halten und für alle Parteien machbar umzusetzen, empfiehlt Tools4ever, das IAM-System in definierten Phasen Schritt für Schritt einzuführen.

Sobald eine Phase erfolgreich abgeschlossen und die neuen Prozesse in der Organisation akzeptiert wurden, kann die nächste Phase eingeleitet werden. Die Schritte, die Ihre Organisation hin zu professionalisiertem Identity & Access Management bewältigen muss, sind unterschiedlich komplex und können z.B. folgendes umfassen:

- Entschluss der Geschäftsleitung für ein zentrales Registrierungssystem aller Identitäten
- Tatsächliche Einrichtung eines Kernregistrierungssystems
- Festlegung der Namenskonventionen

- Harmonisierung von Identitäten in verschiedenen Zielsystemen
- Ausarbeitung und Einrichtung eines umfassenden Access-Governance-Modells mit Rollenprofilen und zugeordneten Berechtigungen
- Verwaltung von Berechtigungen und Umsetzung in der Infrastruktur per Workflow
- Einrichtung eines Self-Service-Portals für Anfrage und Genehmigung zusätzlicher Rechte

Tools4ever weiß aus Erfahrung, dass jeder Schritt mit relativ geringem Aufwand (Tage oder Wochen) technisch implementiert werden kann, dass die Einbettung in die Organisation aber in der Regel aufwendiger ist. Das phasenbasierte Implementierungsverfahren von Tools4ever lässt sich nahtlos in den oben beschriebenen schrittweisen IAM-Reifeprozess Ihrer Organisation integrieren und hat sich über die Jahre bewährt. So kann Tools4ever mit kleinen, gezielten Schritten schnell zur Wertschöpfung in Ihrer Organisation beitragen.

HUNDERTE STANDARD-KONNEKTOREN

Die mangelnde Verfügbarkeit von Schnittstellen zwischen Quell- und Zielsystemen ist ein bekannter Fallstrick bei IAM-Implementierungen. Der Konnektor wird dann vom Implementierungspartner des IAM-Anbieters kundenspezifisch entwickelt. Doch Entwicklung braucht Zeit und wird zudem nicht immer von Fachleuten durchgeführt. Darüber hinaus werden die Weiterentwicklung und der Support für einen spezifischen Konnektor vom IAM-Anbieter oft nicht zugesichert.

Tools4ever ist sehr erfahren in der Entwicklung von Schnittstellen im Bereich IAM und hat bereits über 200 Konnektoren entwickelt. Alle bisher realisierten Konnektoren sind Bestandteil der IAM-Basissoftware und werden dementsprechend unterstützt. Alle Anpassungen der Schnittstellen aufgrund von Änderungen in den Quell- und Zielsystemen sind Teil des Supportvertrags und werden automatisch von Tools4ever umgesetzt und angeboten.

Standardschnittstellen (Auszug)				
HR-Systeme	ADP	Beaufort	Datev	PAISY
	P&I Loga	SAGE	SAP HR	SAP HCM
	Taleo	Youforce		
Krankenhausinformations-systeme (KIS)	McKesson	Meditech	Orbis	ProCare
	SAP for Healthcare			
(Hoch-)Schulinformations-systeme (SIS)	Osiris	Power Campus	Smartschool	SOMtoday
E-Learning	BlackBoard	itslearning	Moodle	
E-Mail-Systeme	Groupwise	Lotus Notes	Microsoft Exchange	Office 365
	Outlook Live	Zimbra		

Service-Management-Systeme	Easylog	HP Service Desk	ServiceNow	TOPdesk
	ZenDesk			
Sicherheits- & Zugangs-systeme	Nedap	Vasco		
Telefonsysteme	Adobe Connect	Avaya	Blackberry	Cisco Call Manager
	Microsoft Lync	Skype for Business		
Facility Management Systeme	Cisco	Facility CMIS	TOPdesk FMIS	
CMS/DMS	DocuShare	LiveLink	SharePoint	Typo3
ERP-Systeme	CODA	Microsoft Dynamics NAV	Oracle eBusiness	SAP
Finanzsysteme	Coupa	Infinium	SAP	
Betriebssysteme	Linux	Powershell	SOAP	Solaris
	Windows			
Datenbanken	FilemakerPro	Oracle	SQL Server	Sybase
Verzeichnis-Dienste	Active Directory	Lotus Notes	Microsoft Azure	Open Directory
	OpenLDAP			
Cloud-Services	Amazon Web Services	Dropbox	Google Apps	Salesforce
Sonstige	Adlib / Axiell ALM	Citrix		

Wenn eine gewünschte Schnittstelle nicht standardmäßig verfügbar ist, wird sie von Tools4ever selbst entwickelt und im Anschluss als Standard-Konnektor in den Identity & Access Manager integriert – mit allen damit verbundenen Vorteilen. Außerdem bietet das IAM-System die Möglichkeit, über ein E-Mail- oder Service-Management-System eine halbautomatische Verbindung einzurichten. In vielen Fällen ist dies eine effiziente (vorläufige) Lösung. Natürlich unterstützt Tools4ever alle Schnittstellenmethoden mit Standard-Protokollen, die üblicherweise für IAM-Systeme verwendet werden.

Standard-Schnittstellenmethoden				
SOAP XML	OpenID	OAuth 2.0	SAML 2	SPML
ODBC	Native Oracle	Progress	SQL Server	CSV

VOLLSTÄNDIGES PORTFOLIO

Der Identity & Access Manager unterstützt Sie sofort bei einer großen Anzahl von User-Lifecycle-Management-Prozessen, die Gartner als Bestandteil einer vollständigen IGA-Lösung aufzählt (*Magic Quadrant for Identity and Access Governance (IGA)* bzw. *Magic Quadrant for User Administration & Provisioning*). Um all diese Anforderungen zu erfüllen, nutzt Tools4ever zusätzliche, selbstentwickelte Software-Produkte, z.B. den *Self Service Reset Password Manager* oder die IDaaS-Lösung *HelloID*, die vollständig mit IAM kompatibel sind. So kann Ihnen Tools4ever ein vollständiges Produktportfolio für Enterprise Identity Governance & Administration anbieten, damit Ihre Organisation keine unterschiedlichen Teil-Lösungen testen und auswählen muss, sondern alles aus einer Hand erhält.

So müssen Sie sich auch keine Sorgen um die Integrationsmöglichkeiten und -unmöglichkeiten machen. Tools4ever hat sämtliche Software von Grund auf selbst entwickelt und nicht nach Übernahmen und Fusionen nachträglich miteinander integriert. In den letzten Jahren ist dieses Vorgehen bei IAM-Anbietern zu einem Trend geworden, der die erfolgreiche Integration, sowie Überlappungen und fehlende Funktionalitäten zu einem großen Problem macht.

SKALIERBARKEIT

Die IAM-Lösung von Tools4ever ist für die Verwaltung sehr großer Organisationen mit zehntausenden Identitäten geeignet, aber genauso auch für kleine und mittlere Betriebe ab 300 Mitarbeitern. Die IAM-Suite enthält verschiedene Komponenten, mit denen kleine und große Organisationen entsprechend unterstützt werden können. So können Sie Ihr Access-Governance-Modell für tausende User ebenso umsetzen, wie sichere Access Policies für Cloud-Anwendungen für wenige Außendienstmitarbeiter.

SICHERHEIT AUS EUROPA

Die Software von Tools4ever wurde und wird vollständig in Europa entwickelt. Alle Server stehen in den Niederlanden. Es werden keinerlei Daten in Drittländer wie die USA übertragen.

REFERENZEN

In den Niederlanden ist Tools4ever mit hunderten IAM-Implementierungen klarer Marktführer. Wettbewerber (FIM, Oracle, Quest, Courion, Okta, Sailpoint, Aveksa, NetIQ) haben dort höchstens ein paar Dutzend Systeme implementiert.

Und auch in Deutschland, Österreich und der Schweiz kann Tools4ever starke Referenzen vorweisen. Wir unterstützen kleine und große Organisationen aus Gesundheitswesen, Industrie, Bildung, Finanzindustrie und Behörden mit der schnellen und reibungslosen Implementierung individuell angepasster Standard-IAM-Lösungen. Bei Problemen steht Ihnen unser internationales Support-Team rund um die Uhr zur Seite. Gerne beraten wir Sie außerdem im Laufe Ihres Implementierungsprozesses zu den *best practices* für Access Governance, Workflow-Management und Compliance.

Auf der Website von Tools4ever finden Sie viele Case Studies von zufriedenen Kunden, die die Erfolgsgeschichte von Tools4ever verdeutlichen. Gerne stellen wir für Sie auch persönlichen Kontakt zu einem passenden Referenzkunden her.

FAZIT

Flexibel, handlungsfähig & innovativ

Auf dem mittlerweile ausgereiften Markt für Identity Governance & Administration kann Tools4ever auf 20 Jahre Erfahrung und eine beeindruckende Erfolgsgeschichte verweisen. Das IAM-Produktportfolio von Tools4ever ist mehr als umfassend und deckt alle Bereiche ab, die Gartner in Berichten zu diesem Thema hervorhebt. Im Vergleich mit Wettbewerbern wie NetIQ / Novell, Oracle, Microsoft, Okta oder Sailpoint ist Tools4ever flexibel, handlungsfähig und höchst innovativ. Wir gehen individuell vor Ort auf Ihre speziellen Anforderungen ein und passen die Standard-IAM-Implementierung nach Ihren Vorstellungen an. Gemeinsam finden wir passende Lösungen für die Herausforderungen in Ihrer Organisation.

Auch wenn die Entwicklung in den Niederlanden stattfindet, können durch das weltweite Netzwerk von Consultants individuelle Anforderungen lokal problemlos umgesetzt und hervorragender Support rund um die Uhr geboten werden. Tools4ever kennt sich mit den länderspezifischen Gesetzen und Verordnungen aus und kann Ihre Organisation entsprechend unterstützen.

Schneller als die anderen

Über die Jahre hat Tools4ever seine Consulting Services perfektioniert. Mit State-of-the-Art-Software, der phasenbasierten Implementierungsmethode und erfahrenen IAM-Consultants ist Tools4ever in der Lage, gebrauchsfertige IAM-Implementierungen durchzuführen – innerhalb von Wochen und nicht, wie auf dem IAM-Markt üblich, innerhalb von Monaten oder Jahren. Das bietet nicht nur uns, sondern ebenso Ihnen einen Wettbewerbsvorteil, denn schon nach wenigen Tagen spüren Sie die Entlastung, die Ihnen der Identity & Access Manager durch Automatisierung von Standardprozessen bietet.

Konkurrenzfähige Preise

Darüber hinaus gilt bei Tools4ever eine sehr wettbewerbsfähige Preispolitik. Die Kombination aus bewiesener Erfolgsgeschichte, bewährter Implementierungsmethode und einer sehr konkurrenzfähigen Preiskalkulation macht Tools4ever zu einem Anbieter, der es wert ist, in die engere Auswahl für Ihre IAM-Lösung aufgenommen zu werden.

Wir bedanken uns für Ihr Interesse an der IAM-Lösung von Tools4ever. Gerne informieren wir Sie über alle Möglichkeiten für Ihre Organisation, etwa mit einer Online-Präsentation, einem Workshop oder einem Proof of Concept (PoC) bei Ihnen vor Ort. Sie erreichen uns über www.tools4ever.de.

TOOLS4EVER Informatik GmbH

Adresse Hauptstraße 145-147
51465 Bergisch Gladbach
Deutschland

Telefon +49 2202 2859-0
E-Mail info@tools4ever.de
Web tools4ever.de

Sales sales@tools4ever.de
Support projectdesk@tools4ever.de