imprivata®
OGiTiX

Ratgeber

IAM VS. ITSM

WIE MAN IAM UND ITSM UNTER EINEN HUT BRINGT

www.ogitix.de

Inhalt

1 Einleitung **3**

2 Identity Access Management **4**

2.1 Was kann IAM? 4

2.2 Neue Anforderungen an IAM-Systeme 5

3 IT Service Management (ITSM) **6**

3.1 Begriffsabgrenzungen: ESM/RBAC 6

4 IAM-Funktionen in der ITSM-Oberfläche? **7**

4.1 Nachteil getrennter Systeme 7

4.2 Was spricht dafür? 7

5 Lücken von ITSM 8

5.1 Schnittstellenkompetenz 8

5.2 Standardfunktionsumfang 8

5.3 Berechtigungsvergabe 9

umfangreicher Berechtigungskatalog 9

fehlende Unterstützung bei der Beantragung von Rechten 10

5.4 Schutz der Privatsphäre 11

5.4.1 Was wird angezeigt? 11

5.4.2 Zugangskontrollen 11

5.4.3 Segregation of Duties 12

5.4.4 Risikobewertungen 12

5.5 Passwort-Management 13

6 Wo ITSM-Prozesse sinnvoll sind **13**

7 Der Königsweg: ITSM und IAM arbeiten integriert zusammen **14**

1 Einleitung

Viele mittlere bis große Unternehmen arbeiten heute mit einer Plattform für IT Service-Management (ITSM) – ServiceNow, BMC Remedy, Ivanti, Atlassian oder MATRIX42 sind bekannte Anbieter in diesem Umfeld. Deren Einsatz zu koordinieren ist schon komplex genug.

Hinzu kommt das Erfordernis, die unterschiedlichen Rollen und Zugriffsberechtigungen im Unternehmen auf die einzelnen Anwendungen und IT-Systeme zu steuern; dafür kommen spezialisierte Softwarelösungen zum Identity Access & Management (IAM-) wie etwa Oneldentity, Sailpoint, Imprivata, Okta oder OGiTiX zum Einsatz.

ITSM-Anbieter und -Beratungshäuser machen sich in jüngerer Vergangenheit dafür stark, Funktionen beider Systeme unter einer einheitlichen Oberfläche bereitzustellen. Auch über das ITSM-System sollen demnach Identitäts- und Zugangsänderungen über ihren gesamten Lebenszyklus hinweg verwaltet werden können.

Auf den ersten Ansatz ein sinnvoller Vorschlag, ganz im Sinne zentralisierter IT und besserer Übersicht. Wie immer aber lauern die Fallstricke im Detail.

Das vorliegende Whitepaper untersucht, in welchen Bereichen eine Verschmelzung unter dem ITSM-Dach funktionieren kann und wo dieser eindeutige Grenzen gesetzt sind. Der Königsweg, so wird sich zeigen, liegt in einem integrativen Zusammenspiel über Schnittstellen.

2 Identity Access Management

2.1 Was kann IAM?

Die IT-Landschaften in den Unternehmen werden heute immer komplexer und sind zunehmend vernetzt, untereinander sowie mit der Außenwelt. Dies macht sie anfällig, für Angriffe von außen ebenso wie für missbräuchliche oder versehentliche Nutzung durch eigene Beschäftigte. Deshalb sollte ein funktionierendes Identity- und Access-Management mittlerweile zum festen Bestandteil der IT-Security-Strategie eines Unternehmens gehören.

Die Realität sieht so aus, dass User heute zumeist mehr Zugangsberechtigungen haben als sie eigentlich benötigen bzw. haben sollten. Aufgabe von IAM-Systemen ist es, diesen Zustand zu bereinigen und die verschiedenen Identitäten innerhalb eines Systems transparent zu verwalten.

Durch Aufsetzen eines Sicherheits-Layers sollen sie für die Etablierung und Einhaltung von Zugangsregeln und -richtlinien sorgen.

Mit IAM können Organisationen Rollen und Zugriffsberechtigungen einzelner User über deren Lifecycle hinweg überwachen sowie workflowgesteuert beantragen, aktualisieren und löschen. Sie können Vorschriften der Berechtigungsvergabe umsetzen und interne Kontrollen automatisieren.

Verlässt eine Person das Unternehmen, wird ihr Zugang zu den internen Softwareanwendungen zuverlässig deaktiviert.

Eine IAM-Lösung stellt sicher, dass neue Zugriffe entsprechend der geschäftlichen Anforderungen und in Übereinstimmung mit den Unternehmensrichtlinien gewährt werden.

Sämtliche Security Policies werden damit eingehalten, in Übereinstimmung mit unternehmenseigenen und externen Compliance-Richtlinien, von der EU-Datenschutzgrundverordnung über BSI KritiV, B3S und Bafin bis hin zu ISO27001, SOX u.a.

Die IAM-Administration überprüft mit IAM-Hilfe regelmäßig die Sicherheitsberechtigungen und entfernt solche, die nicht mehr benötigt werden. Sie kontrolliert den Zugang zu privilegierten Konten und führt eine automatisierte Aufgabentrennung durch. IAM-Lösungen können außerdem das Passwort-Management automatisieren und damit sicherer gestalten sowie insgesamt die Authentifizierungsmechanismen im Unternehmen stärken.

Wo manuelle Prozesse wegfallen, minimieren sich Fehler im Berechtigungswesen (durch versehentlich falsche Eingaben). Die Belastung der Systemadministration sinkt durch Wegfall manueller Routinetätigkeiten und geringeres Anrufvolumen beim IT-Support. Wer bislang ausschließlich im Helpdesk immer wiederkehrende Anfragen abarbeiten musste und durch Audits eingespannt war, kann sich nun strategischen Aufgaben widmen.

2.2 Neue Anforderungen an IAM-Systeme

Seit Mitte der Nullerjahre entwickelt sich das Thema IAM inhaltlich beständig weiter. Anfangs standen Bereiche wie das Passwort-Management, Single Sign-on oder Provisioning im Mittelpunkt. Es folgten Themen wie Identity Federation und Privileged Identity Management.

Inzwischen sind es vor allem der Vorstoß in angrenzende Bereiche wie das IT Service Management bzw. die Abgrenzung demgegenüber, die im IAM-Kontext diskutiert werden.

Bei einer Reihe von ITSM-Anbietern findet man heute Module für Rollen und Berechtigungsmanagement – wenn sie ausgewählte IAM-Funktionen nicht gleich vollständig in ihre IT-Operations-Plattform integrieren.

Es geht im Kern um Genehmigungsprozesse, die beide Sphären verbindet und die eine klare Abgrenzung bzw. Schnittstellendefinition erfordern.
Darin liegt für IAM-Hersteller derzeit die größte Herausforderung.

3 IT Service Management

ITSM-Systeme werden verwendet, um die Bereitstellung von IT-Diensten (und eventuell Nicht-IT-Diensten) im gesamten Unternehmen zu entwickeln, bereitzustellen, zu verwalten und zu optimieren. Sie decken damit die Bereiche Service-Support und Service-Delivery ab; geläufig sind auch die Begriffskategorien Ticket- oder Anfragesystem.

Aufgabe von ITMS-Lösungen ist es, die immer komplexer werdenden Geschäftsprozesse in Unternehmen bestmöglich durch die IT zu unterstützen. Dafür umfassen sie einen Service-Katalog, ein User-Portal für Anfragen (Service Desk), Funktionen für Incident/Asset Management und eine Wissensdatenbank.

ITSM-Frameworks helfen dabei, die jeweils geeigneten Verfahren, Menschen und Technologien so einzusetzen, dass man zu einem optimalen IT–Service-Management gelangt.

Die IT Infrastructure Library (ITIL) gilt als De-facto-Standard für ITSM. Sie stellt verschiedenste Best Practices bereit, mit denen die Qualität des ITSM kontinuierlich verbessert werden kann.
Weitere Frameworks sind COBIT, Six Sigma, Microsoft Operations Framework, ISO 20000 und TOGAF.

3.1 Begriffsabgrenzungen: ESM/RBAC

In jüngerer Vergangenheit ist zudem von Enterprise Service Management (ESM) die Rede, quasi der nächsten Evolutionsstufe des ITSM.
Damit sollen Service-Organisationen in der Lage sein, Daten über die Leistung und das Abschneiden ihrer Business Services zu sammeln und zu analysieren. Es geht praktisch um die Erweiterung des reinen IT Asset Management um Non-IT-Assets, z.B. aus dem Bereich Personalwesen, Finanzen oder Lieferanten-Management.

Auch ITSM-Hersteller reklamieren jedoch für sich, IT- ebenso wie Non-IT-Assets zu verwalten. Der Begriff des ESM bleibt daher strittig.

Unter dem Begriff Role Based Access Control (RBAC) versteht man eine Zugriffskontrolle auf der Basis von Rollen. Das 1992 erstmals beschriebene und 2004 als ANSI-Norm 359-2004 verabschiedete RBAC-Modell soll einem realen User direkt Rechte und Zugriffe auf verschiedene Systeme geben.

Auch steht hier die Benutzerfreundlichkeit im Vordergrund, während sicherheitsrelevante Aspekte vernachlässigt werden.

Das Modell erwies sich jedoch durch die allgemein ansteigende User-Anzahl als unübersichtlich und fehlerträchtig. RBAC hat sich aus diesen Gründen als Begriff in der Breite nicht durchsetzen können.

4 IAM-Funktionen in der ITSM-Oberfläche?

ITSM erlebt derzeit einen Boom und Unternehmen investieren viel Geld und Zeit in die Anschaffung von oder Erneuerung bestehender Lösungen.

Damit drängt sich der Gedanke auf, den Bereich des IAM dort zu integrieren, sprich: beides unter einen Hut zu bringen.

4.1 Nachteil getrennter Systeme

Bei zwei separaten Systemen für ITSM und IAM, so wird argumentiert, seien User wie IT-Admins gezwungen, durch Verlinkungen zwischen den unterschiedlichen Services (Berechtigungen, HR, IT, EDV etc.) „hin- und herzuspringen". Auch die vorgeblich schwere Bedienbarkeit von IAM-Systemen wird als Argument ins Feld geführt.

Moderne ITSM-Systeme verfügten bereits über benutzerfreundliche Anfrageportale, die man durch die Abschaffung der Benutzeroberfläche von IAM-Systemen gleich mitbenutzen könne.

4.2 Was spricht dafür?

Die Idee einer Verschmelzung scheint verlockend. Es gibt große Überschneidungen, betrachtet man allein die Security-Aspekte. IAM stellt sicher, dass die richtigen Personen den passenden Zugriff auf die ihnen zugedachten Ressourcen haben. Dies funktioniert traditionell über Passwörter. Und 40 Prozent der Kontakte mit dem IT-Servicedesk beziehen sich auf genau deren Zurücksetzen und damit auf einen Kernbereich von IAM!

Ein einziges Portal soll Prozesse vereinfachen, über Self-Service-IAM Zeiten des Helpdesks reduzieren, die dieser zum Schließen von Tickets benötigt, und für mehr Effizienz sorgen.

Als grundlegende Vorteile, wenn man IT-Anfragen (auch solche aus dem IAM) in das ITSM überträgt, werden genannt:

- ➔ One-Stop-Shopping für Benutzer
- ➔ weniger Plattformen, welche die IT-Abteilung verwalten muss
- ➔ Besserer Überblick, wo Ressourcen über verschiedene Dienste hinweg verbraucht werden

5 Lücken von ITSM

IAM-Funktionen einfach in die ITSM-Oberfläche einzubauen, funktioniert allerdings nicht so ohne weiteres. Dagegen spricht eine Reihe von Gründen:

5.1 Schnittstellenkompetenz

IAM- wie ITSM-Systeme sind darauf ausgelegt, die Bereitstellung von Software- Anwendungen zu gewährleisten bzw. der Zugriff auf diese zu regeln. Sie müssen folglich in der Lage sein, all diese produktiven Anwendungen anbinden zu können. An genau dieser Schnittstellenkompetenz mangelt es jedoch ITSM-Systemen. Sie haben vom Ansatz her eher Ticket/Service-Request-Charakter und wurden nicht originär dafür entwickelt, um zu automatisieren, zu orchestrieren und provisionieren.

IAM-Systeme hingegen konzentrieren sich von Beginn an auf Prozesse wie Eintritte, Wechsel- und Austrittsprozesse und die Automation.

Sie bringen daher grundsätzlich standardisierte Schnittstellen zu angrenzenden Systemen mit. In ITSM-Systemen müssen diese i.d.R. erst aufwändig eingerichtet werden.

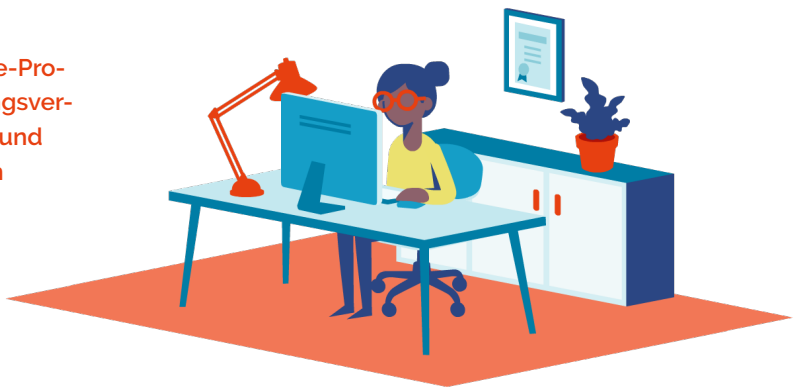
Gute IAM-Lösungen bieten beispielweise **Standardschnittstellen für HR-Quellen** wie SAP HCM, Loga oder Workday sowie für Zielsysteme wie Active Directory, SAP, M365, KIS, Exchange, Teams u.v.m.

5.2 Standardfunktionsumfang

IAM lässt sich in Ansätzen über ITSM-Systeme abbilden, jedoch verfügen die wenigsten von ihnen über fertige IAM-Prozesse und -Funktionen. Der Reifegrad der Standards (sofern solche vorhanden sind) und die Lösungstiefe sind im ITSM-Umfeld unterentwickelt, das meiste muss zunächst gecustomized werden.

IAM-Systeme hingegen bilden die Lifecycle-Prozesse eines Beschäftigten, die Berechtigungsvergabe, Self-Services, 4-Augen-Prinzip, Ziel- und Quellsystem-Orchestrierung etc. bereits im Standard über fertige Prozesse ab.

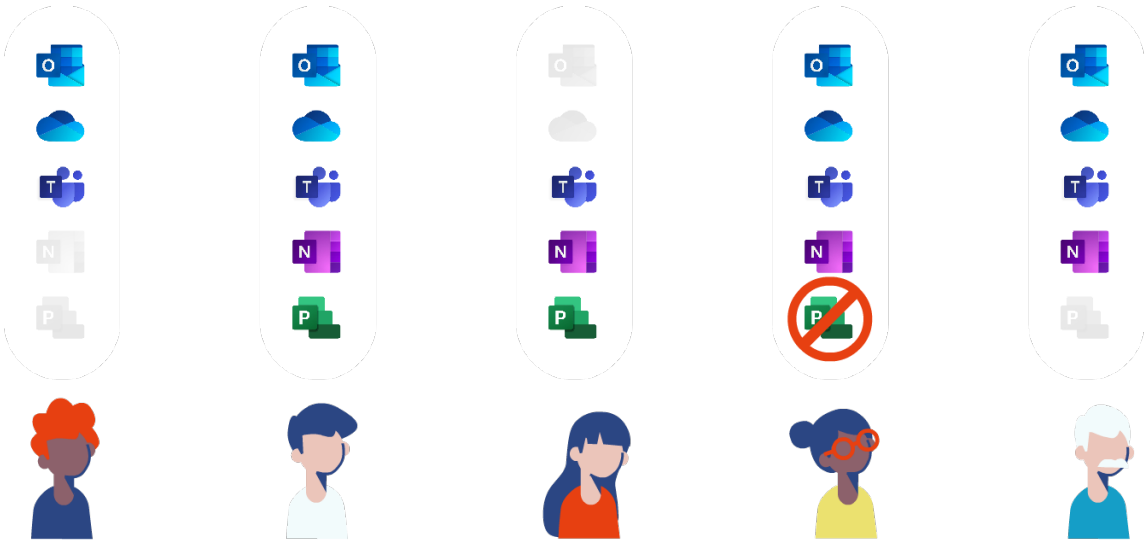
Hersteller-Support, Release-Management werden out-of-the-box mitgeliefert. IAM-bezogene Aufgaben lassen sich dadurch viel schneller umsetzen.



5.3 Berechtigungsvergabe

Aufgrund bestimmter Merkmale kann man Personen aufgrund ihrer Stellung zum Unternehmen (z. B. Angestellter oder Auftragnehmer) oder Rolle (z. B. Verkäufer:in) automatisch antizipierbare Rechte zuweisen. Im IAM wird deshalb unterschieden zwischen vorhersagbaren Berechtigungen auf der einen Seite und beantragten auf der anderen.

Die Herausforderung liegt darin, dass nicht alle Berechtigungen vorhersehbar sind – alles andere muss angefordert werden.



Umfangreicher Berechtigungskatalog

Der typische gemeinsame Berechtigungskatalog einer auch nur mittelgroßen Organisation kann Millionen von anforderbaren Zugangsrechten enthalten.

Beispiele:

- 100 SAP-Instanzen x je 4000 Rollen = **400k Berechtigungen**
- 3 Active-Directory-Domänen x 10.000 Gruppen = **30k Gruppen**

Aus einem derart großen Menü von Optionen die richtigen Berechtigungen auszuwählen, ist schlichtweg unmöglich.

Ein User A wird daher den Weg des geringsten Widerstands gehen und über den ITSM-Helpdesk beim IT Support anfragen, ihm die gleichen Rechte zu erteilen wie User B aus der gleichen Abteilung. Das hat schwerwiegende Folgen für die IT-Sicherheit.

Hat B schon jetzt zu viele Rechte, dann hat A diese künftig auch.
Ungeklärt bleibt außerdem, ob A wirklich alle Rechte braucht, die B hat.

Fehlende Unterstützung bei der Beantragung von Rechten

An dieser Stelle unterstützen IAM-Systeme die antragstellende Person bei der Auswahl von Berechtigungen – eine der Basis-Fähigkeiten moderner IAM-Systeme, die sie grundlegend von ITSM-Lösungen unterscheiden. Hierbei gibt es mehrere, sich ergänzende Strategien:.

Beispiele:

- Zusammenfassen von Berechtigungen in Rollen
- Suche nach Berechtigungen anhand der Beschreibung oder Metadaten-Tags
- Abfangen von „Zugriff verweigert"-Fehlern und Weiterleitung der Benutzer zur Anfrageseite (insbesondere unter Windows und SharePoint)
- Vergleich von Modell- und Empfängerbenutzern und Auswahl der zu kopierenden Elemente
- Empfehlen von Berechtigungen, die in der Gruppe des Antragstellenden üblich bzw. beliebt sind

Defizit eines ITSM-Systems bei der Rechtevergabe ist es also, dass kein integrierter Berechtigungskatalog vorliegt.
Ein IAM-System müsste ihm diesen erst tagesaktuell über eine Integration einspeisen. Es gibt ferner kein Rollenkonzept (einige ITSM-Anwendungen könnten dies allerdings als Sammlungen von Services im Katalog modellieren) sowie keine Berechtigungs-Metadaten (könnten modelliert werden, was aber Aufwand bei der Definition von Formularen und Workflows bedeutet).

Während die vorgenannten Defizite noch (wie beschrieben) ausgeglichen werden können, sind die folgenden schwerwiegender: ITSM haben keinen Mechanismus, um Fehler bei verweigertem Zugriff abzufangen. Sie können nicht darstellen, wer bereits welche Zugriffsrechte hat. Und sie können Berechtigungen zwischen Benutzern nicht vergleichen.

Fazit: Die Beantragung von inkrementellem Zugriff über ITSM lässt sich nicht benutzerfreundlich gestalten.

5.4 Schutz der Privatsphäre

Der Schutz der Privatsphäre ist bei IAM-Systemen, anders als bei ITSM, ein eingebauter Mechanismus. Darüber werden folgende Sachverhalte geregelt:

5.4.1 Was wird angezeigt?

Ob User A im System den Datensatz von User B einsehen darf, hängt davon ab, wie beide miteinander verbunden sind. Welche passenden User werden angezeigt, wenn A nach Usern sucht, die Kriterium C entsprechen?

Solche Kontrollen sind nicht verhandelbar – ihr Versagen bedeutet ein eklatantes Risiko für die Einhaltung von Datenschutz-Richtlinien.

5.4.2 Zugangskontrollen

Welche Art von Änderungen User A im Namen von B beantragen kann, hängt von der Beziehung zwischen A und B ab (Führungskraft/Teammitglied, HR/Arbeitgeber, IT-Support/Anrufer).
Ein IAM-System regelt, wer aufgefordert werden soll, Anträge zu genehmigen: der (derzeitige oder vorgeschlagene/neue) Vorgesetzte des Empfängers, der Vorgesetzte des Antragstellers oder ggf. eine für die Ausbildung verantwortliche Person?

Durch alleinigen Einsatz von ITSM-Systemen ist es nicht möglich, den Zugriff auf der Grundlage der Beziehungen zwischen Anforderer/Empfänger/Berechtigter zu kontrollieren.

5.4.3 Segregation of Duties

Eine Kernkompetenz von IAM, die sich durch ITSM nicht abbilden lässt, ist die die Trennung von Zuständigkeiten (Segregation of Duties = SoD). Darüber wird geregelt, dass bestimmte verbotene Kombinationen von Berechtigungen nicht zugelassen werden: **Jemand, der Zugang auf A hat, darf ihn nicht auch auf B haben.** Generell sollten keinem User mehr als n von m Berechtigungen zugewiesen werden.

IAM-Systeme definieren Rollen, die Gruppen und andere Rollen enthalten. Es existiert eine ganze Hierarchie von Berechtigungen. SoD-Verletzungen entstehen oft auf einer anderen Ebene der Berechtigungshierarchie als dort, wo eine Regel definiert wurde.
Bei der Bewertung von Richtlinien unterscheidet IAM zwischen zugewiesenen, zuvor angeforderten, aber noch nicht zugewiesenen sowie neu angeforderten Berechtigungen.
Auch genehmigte Ausnahmen von SoD-Regeln werden über IAM gesteuert.
IAM spürt User auf, die bereits gegen SoD-Regeln verstoßen und stellt vorbeugend sicher, dass Zugriffsanfragen keine neuen Verstöße auslösen.

Komplex wird die Angelegenheit durch verschachtelte Zugangsrechte. Denn „Berechtigungen" ist normalerweise nur eine Umschreibung für „Gruppenmitgliedschaften"; Gruppen auf einigen Systemen (AD, LDAP) können ferner andere Gruppen als Mitglieder enthalten.
Gerade in Kombination mit verschachtelten Berechtigungen hat sich gezeigt, dass SoD nicht oder nur sehr aufwändig in die benutzerdefinierte Anwendungslogik eines ITMS-Systems zu implementieren ist.

5.4.4 Risikobewertungen

Anders als ITSM-Systeme können IAM-Lösungen anzeigen, welches Risiko für die Organisation von einem bestimmten User ausgeht. Indizien dafür liegen vor, wenn dieser eine Richtlinienverletzung begangen hat.

Auch wenn jemand viele Beschäftigte unter sich hat oder in Hochrisikobereichen des Unternehmens arbeitet, kann ein Verdachtsmoment vorliegen.

Solche Personen kann das IAM-System einer besonderen Behandlung unterziehen – etwa der Art, dass wenn sie neue Rechte beantragen, die Freigabe zusätzliche Schleifen durchläuft oder vergebene Rechte in engerem zeitlichen Abstand kontrolliert bzw. rezertifiziert werden.

Fazit: Die Beantragung von inkrementellem Zugriff mit ITSM-Tools ist unsicher und genügt nicht den allgemeinen Anforderungen an den Schutz der Privatsphäre.

5.5 Passwort-Management

ITSM-Systeme werden in der Regel vom IT-Helpdesk angeschafft, dessen häufigste gemeldete Fälle Login-Fehler sind. Kann über ITSM das Problem vergessener/gesperrter Passwörter hinreichend gelöst werden?

Passwort-Management, eine der Kernkompetenzen von IAM, ist weit mehr als eine Webanwendung, wie man sie vom Self-Service-Password-Reset kennt. Dieser sollte auch über den Anmeldebildschirm des eigenen Rechners möglich sein. Es muss außerdem möglich sein, Passwörter nicht nur über das Netzwerk wiederherzustellen, sondern lokal im Cache gespeicherte Passwörter nach einem Reset zu aktualisieren. Passwort-Verwaltung umfasst ferner das Entsperren von Benutzern, die ein per-Boot-Passwort vergessen haben, welches ein verschlüsseltes Laufwerk entsperrt – Fähigkeiten, die kein heutiges ITSM-System aufweist.

6 Wo ITSM-Prozesse sinnvoll sind

Anhand verschiedener Kriterien wurde in den vorangegangenen Abschnitten erläutert, wo ITSM-Systeme ihre Grenzen haben, wenn es um einen professionelles Berechtigungsmanagement geht. **Demnach eignen sie sich für IAM-Zwecke nur sehr eingeschränkt: wenn der Schutz der Privatsphäre keine Rolle spielt, der Berechtigungskatalog nicht betroffen ist und man es mit einfachen Zugangskontrollen sowie Genehmigungsprozessen zu tun hat.**

In Unternehmen mit einem hohen ITSM-Reifegrad kann das Service-Management ein probates Werkzeug für bestimme Prozesse wie Antrag- und Genehmigungen oder auch teilweise für Lifecycle-Prozesse wie Neueinstellungen, Versetzungen oder Austritte sein. Dies setzt jedoch ein integriertes oder angebundenes Organisationsmanagement voraus. Es ist auch dann im IAM-Kontext nur eine Teillösung, da Rollen und Provisionierung, wenn überhaupt, nur rudimentär enthalten sind.

7 Der Königsweg: ITSM und IAM arbeiten integriert zusammen

Sowohl ITSM als auch IAM sind wesentliche Bestandteile einer IT-Infrastruktur. Unternehmen brauchen beide Systeme, da jedes speziell ihm zugedachte Zwecke erfüllt. Sie sollten daher integriert und in einer Art und Weise miteinander kombiniert werden, dass Anfragen und Status-Updates zwischen ihnen ausgetauscht bzw. navigiert werden können.

Einfache Anfragen können ihren Ursprung im ITSM haben, wenn sie nicht den Datenschutz und Privacy Policies betreffen, keine komplexe Autorisierung erfordern, die User keine Hilfe bei der Auswahl aus vielen Berechtigungen benötigen und auch keine Trennung der Zuständigkeiten erforderlich ist. Alles was in punkto Komplexität und Sicherheit darüber hinaus geht, sollte über das IAM geregelt werden. Ein Spezialfall, der von den aktuellen ITSM-Produkten nicht abgedeckt wird, ist das Passwort-Management.

Damit stellt sich die Frage, welche Möglichkeiten und Best Practices der Anbindung für einen kombinierten Einsatz es gibt. Dies bemisst sich vor allem an der Reife und Einsatztiefe des jeweiligen ITSM-Systems.

- **Stufe eins** geht vom klassischen Einsatz des ITSM als Ticketsystem aus.
  Für jegliche manuell zu erledigenden Aufgaben, die im Zuge von IAM entstehen, erstellt die IAM-Software automatisiert ein Ticket, das anschließend im ITSM auftaucht und über dieses abgearbeitet wird. Die IAM-Aktivitäten werden im ITSM dokumentiert; dieses hat damit die Aufsicht über alle IT-Services, einschließlich der IAM-Anfragen
- **In Stufe zwei** wird das ITSM als Ticketsystem inkl. User-Portal verwendet.
  In dieses Portal werden dann IAM-Formulare und Berichte integriert, so dass der User gefühlt nur ein Portal für seine Anfragen und Service Requests benötigt. Auch wenn im Hintergrund zwei unterschiedliche Softwaresysteme agieren und die Abarbeitung übernehmen.
- **ITSM des Reifegrades 3** beinhalten zusätzlich zum Portal auch die Prozesse und Daten für automatisierte Antrag- und Genehmigungsprozesse.
  IAM und ITSM werden in diesem Integrationsszenario bidirektional über eine Schnittstelle integriert und sorgen auch für eine dauerhafte Synchronisierung von Genehmigungsstrukturen. Die Genehmigungsprozesse im Zuge ITSM- und IAM-Prozesse werden bei diesem Szenario durch die ITSM abgewickelt.
- **Die letzte Stufe vier** sähe so aus, dass das ITSM als zentrales Werkzeug betrachtet, d.h. auch als zentrales Portal für alle IT-relevanten Anfrage genutzt wird.
  Dies umfasst dann auch Geschäftsprozesse wie den Identitätslebenszyklus, synchronisierter HR-Daten und Organisations-Management. Das IAM fungiert in diesem Falle nur noch „im Hintergrund“ als reine Middleware für Rollen, Provisionierung und De-Provisionierung.

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