

Vom IAM-Tool zum User-Management-Prozess

Sicherer Benutzerzugang

Zur Verwaltung aufgabenbezogener Zugriffsrechte von Mitarbeitern in Unternehmen und ihrer wechselnden aktiven und inaktiven Rollen kommen IAM-Systeme (Identity- and Access-Management) zum Einsatz. Die Projekte scheitern jedoch häufig an der Konzeption als reine IT-Projekte. Ein neuer Ansatz geht dagegen von einem User-Management-Prozess aus, der lediglich softwaregestützt ist: Die Prozesse definieren die Anforderungen an die IT-Lösung.

Die Nutzung von IT-Applikationen ist heute aus dem Arbeitsalltag der unterschiedlichsten Unternehmensbereiche kaum wegzudenken. Mit steigender Anzahl der genutzten IT-Anwendungen steigt auch die Komplexität der IT-Infrastruktur. In vielen Unternehmen ist durch den Ein-

nuell oder nur zum Teil automatisiert, was hohe Kosten wie auch eine hohe Fehleranfälligkeit verursacht. Die Verantwortung für das Access-Management im Unternehmen ist meist verteilt oder gar ungeklärt. Compliance-Anforderungen und Gesetze wie der Sarbanes-Oxley Act (SOX) und

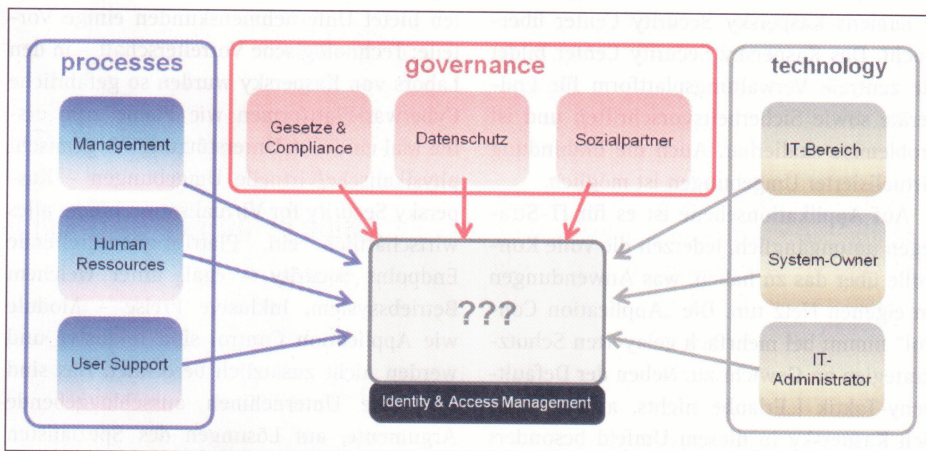
nes konzernweiten Identity- und Access-Managements im Unternehmen. Folgende Ziele sind dabei zu erreichen:

- die Definition und Abstimmung konzernweit einheitlicher Prozesse für die automatisierten Abläufe der Identitäts- und Berechtigungsverwaltung,
- die Erfüllung von Compliance- und Security-Anforderungen für interne Kontrollsysteme,
- die Konzeption und der Aufbau einer zentralen IT-Lösung für das Management von IT-Berechtigungen sowie
- die Anbindung geschäftskritischer Applikationen an eine zentrale, qualitätsgesicherte Benutzerverwaltung.

IAM-Prozesse wurden sukzessive entwickelt, um den wachsenden Compliance- und Governance-Anforderungen Rechnung zu tragen. Das IAM der Unternehmen besteht in der Regel aus einer technischen IAM-Lösung, deren Architektur historisch mit der Komplexität des Unternehmens gewachsen ist. Wenn in einer Geschäftsanwendung ein Problem auftaucht, setzen die üblichen IAM-Lösungen punktuell am betroffenen System an und versuchen, das Problem mit einem Governance- oder einem technisch ausgerichteten Ansatz zu beheben. Ein neuer Ansatz besteht darin, an den übergeordneten Prozessen anzusetzen, um eine nachhaltige Lösung zu finden.

Prozessansatz

Die optimale Lösung ist für jedes Unternehmen auf Basis des vorhandenen Know-hows zu erarbeiten. Dazu sind im ersten Schritt alle Stakeholder im Unternehmen von der Rechtsabteilung über HR (Human Resources, Personalwesen) bis zur IT zusammenzubringen, um gemeinsame Anforderungen, Ziele und Vorgehensweisen zu vereinbaren. Die Rollenstrukturen im Unternehmen basieren auf den unternehmensspezifischen Geschäftsprozessen. Der Fokus für das IAM liegt dabei auf den HR-Prozessen zur Ermittlung des Zusammenhangs zwischen Eintritt, Wechsel und Austritt eines Mitarbeiters und den damit einhergehenden Vorgängen in den IT-Applikationen. Der Schwerpunkt liegt hier auf der Konzeption von Prozessen zur Vergabe und Prüfung sowie dem Entzug



Zahlreiche Seiten stellen Anforderungen an das Identity- und Access-Management im Unternehmen.

Bild: Punktgenau Business Consulting

satz diverser IT-Lösungen eine heterogene Business-Applikationslandschaft mit unterschiedlichen Arten der Benutzerverwaltung entstanden. Das Ergebnis: eine redundante Datenhaltung sowie ein unregelmäßiger Datenabgleich zwischen den Systemen, sofern er überhaupt vorhanden ist. Die IT-Administrationsprozesse erfolgen ma-

das Gesetz zur Modernisierung des Bilanzrechts (BilMoG) stellen jedoch hohe Anforderungen an interne Kontrollsysteme. Auch die internen Sicherheitsbestimmungen zwingen dazu, den vorhandenen Wildwuchs durch ein zentrales und dokumentierbares Management zu ersetzen. Ein Lösungsansatz ist die Einführung ei-

von Berechtigungen, basierend auf den Ereignissen im „User Lifecycle“ (Dauer des Arbeitsverhältnisses). Um diese Prozesse nachhaltig im Unternehmen zu etablieren, ist die Einbindung aller Anforderungen entscheidend.

Aus den Unternehmensprozessen lassen sich Auslöser ableiten, die Änderungen von IT-Berechtigungen bewirken. Diese Analyse bietet eine prozessorientierte Grundlage für die Anforderungen an die IAM-Lösung. Sie dokumentieren demnach die Soll-Vorgänge des IAM-Systems. Zwingende Rahmenbedingungen stellen dabei auch die Anforderungen an Datenschutz und Compliance dar. Gleichzeitig gilt es, das Umfeld im Unternehmen aufzubauen, um die neuen Prozesse zu implementieren, die erforderliche Basisdatenqualität zu schaffen und Pilotapplikationen an die IT-Lösung anzuschließen. Die Prozesssicht wird in diesem Sinne von der Idee bis zur Implementierung und Transition in den Betrieb übernommen.

Das Identity- und Access-Management erhält dadurch neue Schwerpunkte: Während früher der Fokus auf der individuellen Rechtevergabe lag, sind heute einerseits Datenschutz und Compliance und andererseits Rollenmodelle und User-Lifecycle-Prozesse in den Vordergrund gerückt. Eine IAM-Lösung besteht damit aus den folgenden Bestandteilen:

- Die User-Lifecycle-Prozesse enthalten HR-fokussierte Prozesse zur Verwaltung und Betreuung der Berechtigungen der Mitarbeiter.
- Die technischen Prozesse beinhalten Rechtevergabe, -kontrolle und -bewertung sowie Datenverwaltung.
- Die Identity-Management-Lösung besteht im Idealfall aus einem zentralen technischen System.
- Das Access-Management besteht typischerweise aus mehreren technischen Modulen und gliedert sich nach technischen Lösungen, zum Beispiel LDAP und SAP.

Daneben lässt sich mit den IAM-Services Single Sign-on (SSO) und User Self-Service (USS) auch die Produktivität und die Akzeptanz der Unternehmens-IT bei den Anwendern steigern. Denn Anwender

wollen nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die sie berechtigt sind, zugreifen können, ohne sich an jeder Anwendung neu anmelden zu müssen. Ziel von SSO ist es, dass sich die Benutzer nur einmal authentisieren, zum Beispiel zertifikatsbasiert. Danach übernimmt der SSO-Mechanismus die Aufgabe, die erkannte Identität an den Geschäftsanwendungen zu authentifizieren. USS wiederum ermöglicht es dem Benutzer, seine eigenen Daten – zum Beispiel Telefonnummer und Standort – zu pflegen sowie IT-Passwörter zurückzusetzen oder zu ändern.

Ergebnis und Nutzen

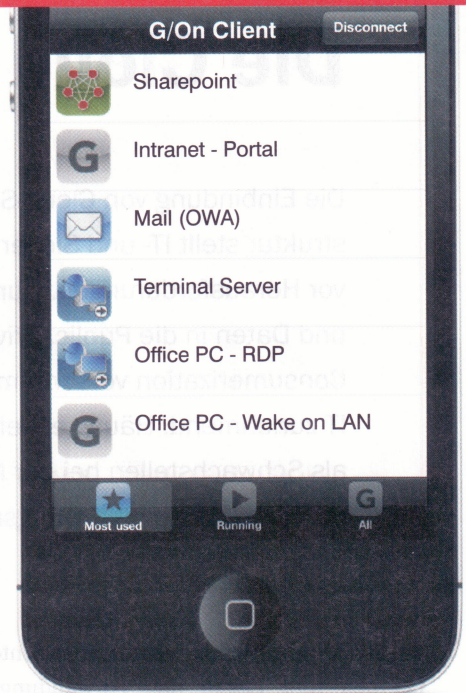
Ein wesentliches Ergebnis der Prozessorientierung ist die Harmonisierung der IT- und der vorgelagerten HR-Abläufe. Dies reduziert die Ausgaben durch sinkenden Kosten für die IT-Administration, den Wegfall manueller Vorgänge sowie eine automatische Fehleranalyse und -behebung. In der Folge verringern sich auch die Kosten für Helpdesk und Support.

Die eindeutige Zuordnung von Identitäten und Arbeitsverhältnissen zu Mitarbeitern erhöht die Transparenz, und die IT-Berechtigungen werden regelmäßig automatisch kontrolliert. Gleichzeitig befolgt ein Unternehmen damit die aktuellen Datenschutz- und Sicherheitsanforderungen sowie Sicherheitskonzepte, während es die Berechtigungsvergabe unter Berücksichtigung der Funktionstrennung automatisiert. Die schnelle Aktivierung von Zugängen erhöht die Arbeitsfähigkeit und steigert in der Folge die Effizienz im Unternehmen. Der neue Ansatz sieht vor, die zentrale Verwaltung von Identitäten und IT-Berechtigungen prozessgesteuert als „Secure-User-Management“ aufzusetzen. Der individuelle IAM-Ansatz wird auf Basis der unternehmensinternen Abläufe konzipiert und in die IT-Infrastruktur eingebettet. Als Ergebnis kann ein Unternehmen die Arbeitsprozesse Compliance-konform ausrichten und standardisieren.

Eugenia Jun/wg

Eugenia Jun ist Senior Consultant bei Punktgenau Business Consulting.

G/On™



Bring Your Own Device Vergessen Sie VPN... und gut.

- keine veraltete VPN-Technik
- vollständige Netztrennung
- exklusive 1:1 Kommunikation
- 100 % geräteunabhängig
- maximale Skalierbarkeit
- außergewöhnlich einfach
- sofortige Kostensenkung

G/On Virtual Access unterstützt
Windows · Linux · Mac OS X · iOS

Success Stories,
Videoclips und mehr
finden Sie online auf
www.giritech.de

