IBM Software Group

Effektive Governance für Identitäts- und Zugriffsmanagement



Juni 2009

Effektive Governance für Identitäts- und Zugriffsmanagement

Heutzutage müssen Unternehmen viele Hürden überwinden, um konsistente Rentabilität zu erzielen und organisatorische Risiken zu bewältigen. Compliance-Verordnungen wie Sarbanes-Oxley, Basel II, Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Model Audit Rule (MAR) und Payment Card Industry Data Security Standard (PCI/DSS) vergrößern diese Herausforderungen noch: Sie erfordern Prozesse und Kontrollen, die in der Regel auf branchenspezifische Ziele ausgerichtet sind.

Die mit der Erfüllung der Compliance-Anforderungen verbundenen Kosten behindern auch die Gewinnziele des Unternehmens; die Verwaltung des Informationslebenszyklus bedeutet aus folgenden Gründen eine erhebliche finanzielle Belastung:

- *Explosionsartiges Wachstum strukturierter und unstrukturierter Daten*
- *Allgegenwärtiger Zugriff auf Informationen*
- *Zunahme vielfältiger, internetbasierter Zusammenarbeit*

Die Implementierung einer kohärenten Strategie zur Zugriffssteuerung und zur Verhinderung von Daten- und Informationsverlust ist eine schwierige Aufgabe, da die Zugriffskontrollen sich auf die gesamte Struktur von IT und Rechenzentrum erstrecken und zugleich in das unternehmensweite Risikomanagement integriert werden müssen. Unzureichende Transparenz, ineffektive Kontrollen und steigender Verwaltungsaufwand hindern ein Unternehmen daran, sein Kerngeschäft wahrzunehmen und neue Services zur Umsatzgenerierung bereitzustellen. Unternehmen benötigen ein strategisches Konzept, um sich ein Bild von ihren digitalen Identitäten zu machen und sich den Herausforderungen zu stellen, die Verwaltung, gemeinsame Nutzung und Überprüfung von Identitäten und Berechtigungen[1] mit sich bringen.

Governance, Risikomanagement und Compliance zählen zu den wichtigsten Geschäftsaufgaben

Die Kontrolle des Zugriffs auf Daten und Anwendungen ist von essenzieller Bedeutung. Steigende Sicherheits- und Datenschutzbelange und ein stärkerer Fokus auf unternehmensweiter Aufsicht machen Governance, Risikomanagement und Compliance (GRC) zu den wichtigsten Geschäftsaufgaben. Unternehmen müssen nachweisen, dass sie über starke und konsistente Zugriffssteuerungen verfügen.

„Identity and Access Management Governance“ (IAM-Governance) beschreibt, wie Unternehmen die Identitäten und den Zugriff auf Anwendungen, Informationen und Systeme verwalten, schützen und überwachen. Sie vergrößert den Nutzen der zentralen Identitäts- und Zugriffsmanagementfunktionen wie Benutzereinrichtung, Webzugriffsmanagement und Verzeichnisinfrastruktur. Das vorliegende White Paper betrachtet verbreitete, wenn auch fragmentierte Strategien für IAM-Governance sowie den IBM Ansatz, der auf alle Anforderungen der IAM-Governance ganzheitlich eingeht.

Wahl eines richtlinienbasierten Ansatzes für die Verwaltung von Personen, Anwendungen und Daten

Unternehmen sollten einen umfassenden Ansatz für IAM-Governance ins Auge fassen, der folgende Anforderungen erfüllt: Erkennung, Dokumentation und Analyse des Benutzerzugriffs; Einführung eines Prozesses zur Regelung des Benutzerzugriffs; Bewältigung von Geschäftskonflikten mithilfe von Einschränkungen; Durchsetzung von Richtlinien; kontinuierliche Überwachung.

Ein derartiges Konzept sollte die Mitarbeiter aus IT und Geschäftsbereich mit automatisierten Verfahren zur Identifizierung, Bereinigung und Zuordnung von Identitätsdaten ausstatten; Identitäts- und Berechtigungsdaten anwendungsübergreifend in einem wiederverwendbaren, praxistauglichen Format erkennen, klassifizieren und analysieren, um die Erstellung von Rollen[2] zu vereinfachen; und Rollen, Identitätsattribute[3] und Berechtigungen für die gesamte Nutzungsdauer definieren und verwalten.

Weitere essenzielle Elemente einer effektiven IAM-Governance:

- *Eine Ebene der Richtliniengovernance, die auf kontrollierte Weise und zentral auf Geschäfts- und IT-Richtlinien angewendet wird*
- *Eine Ebene der Richtliniendurchsetzung und -korrektur zur Automatisierung von Workflows, Aufgaben und Prozessen*
- *Überwachung, Berichterstellung und Prüfung, um den korrekten Einsatz der Zugriffsrechte sicherzustellen und um sowohl in die Richtliniengovernance als auch in die Identitäts- und Rollenstruktur des Unternehmens Rückmeldungen einfließen zu lassen*

Ein richtlinienbasiertes Konzept, das die richtige Lösung einsetzt, sorgt für die erforderliche Transparenz, Kontrolle und Automation, um geschäftsspezifische Benutzerzugriffsanforderungen mit höherer Zurechenbarkeit zu verwalten und die Regelung und Durchsetzung des Zugriffs sicherzustellen.

Weitere Informationen

Weitere Informationen zur Entwicklung einer ganzheitlichen IAM-Governance-Strategie erhalten Sie bei Ihrem IBM Ansprechpartner oder IBM Business Partner oder auf folgenden Websites:

- **ibm.com**/tivoli/products/identify-access-assurance
- **ibm.com**/tivoli/products/identity-mgr
- **ibm.com**/services/gbs
- **ibm.com**/services/us/index.wss/offering/iss/a1030826

Informationen zu IBM Service Management

IBM Service Management-Lösungen unterstützen Unternehmen bei der Verwaltung ihrer Geschäftsinfrastruktur und bei der Bereitstellung eines hochwertigen Service, der effektiv gesteuert wird und den Benutzern, Kunden und Partnern unterbrechungsfrei und sicher zur Verfügung steht. Unternehmen aller Größenordnungen können IBM Services, Software und Hardware für Planung, Ausführung und Management von Initiativen für Service- und Ressourcenmanagement, Sicherheit sowie Hochverfügbarkeit und Ausfallsicherheit von Geschäftsanwendungen und -prozessen nutzen. Flexible, modulare Angebote decken die Betriebssteuerung, die IT-Entwicklung, die Ressourcenverwaltung und die Systemverwaltung ab und basieren auf umfangreichen Erfahrungsberichten von Kunden, auf bewährten Verfahren und auf Technologien auf der Grundlage offener Standards. IBM agiert als strategischer Partner, um die Kunden bei der Implementierung der richtigen Lösungen zu unterstützen, die für schnellen Geschäftserfolg und ein schnelleres Unternehmenswachstum sorgen.

[1] *Berechtigung – Zugriffsrechte für Anwendungen, Services oder Daten, etwa die Berechtigung, auf die SAP-Finanzanwendung zuzugreifen oder die Finanzdatensätze der Kundendatenbank zu ändern.*

[2] *Es gibt verschiedene Typen von Rollen. Geschäftsrollen entsprechen Benutzergruppen (z. B. Finanzanalysten), Anwendungsrollen entsprechen Gruppen von Ressourcen oder Berechtigungen (z. B. „Kaufauftrag genehmigen").*

[3] *Identitätsattribut – ein Datenelement, das mit Benutzern verknüpft ist, etwa Jobcode, Abteilungsnummer usw.*

Inhalt

Aktuelle Produkte bilden einen fragmentierten Ansatz

Der heutige Markt für IAM-Governance ist fragmentiert; es gibt Einzelprodukte für Zugriffszertifizierung, Aufteilung von Aufgabenbereichen, Rollenmanagement, Berechtigungsmanagement und Privileged-Identity-Management – Produkte, die nicht ganzheitlich auf die Anforderungen der IAM-Governance eingehen.

Erfüllung jeder Anforderung der IAM-Governance

Unter dem Druck von GRC und der Notwendigkeit, Informationen an viele Beteiligte weiterzugeben, müssen Unternehmen jede Anforderung der IAM-Governance erfüllen:

1. Die richtigen Informationen zur richtigen Zeit und zum richtigen Zweck an die richtigen Personen weitergeben.

2. Richtlinien und Verordnungen auf Geschäftsoperationen anwenden.

3. Dokumentation der Benutzerzugriffe auf kritische Prozesse, Informationssysteme und Daten sollte als grundlegende Risikomanagementkontrolle verwaltet werden.

4. Den Grad des Zugriffs erfassen, den Benutzer auf Services, Anwendungen und Daten haben. Sicherstellen und dokumentieren, dass der Benutzerzugriff ein berechtigtes Geschäftsinteresse hat und Konflikten bei der Aufteilung von Aufgabenbereichen vorbeugt.

5. Governance über physische und logische Zugriffsberechtigungen[4] definieren und verwalten, einschließlich eines Zertifizierungsvorgangs, der für gültigen Benutzerzugriff und gegebenenfalls für dessen Widerruf sorgt.

6. Governance mit Zurechenbarkeit, Verwaltbarkeit, Nachhaltigkeit und Dokumentation für Rechtsinhaber aus Geschäftsbereich und IT implementieren und Delegierungen zulassen. Eine Vereinbarung zwischen Geschäftsbereich und IT entwickeln, die festlegt, wie die IT diesen Prozess effektiv und wiederholt verwalten kann, während der Geschäftsbereich die Zugriffsverantwortlichkeit beaufsichtigt.

7. Eine systematische IT-Architektur und -Plattform dazu nutzen, die Richtlinien konzeptionsgemäß durchzusetzen und Rückmeldungen zur Verfügung zu stellen, damit sowohl dem Geschäftsbereich als auch der IT die Ergebnisse fortlaufender Compliance innerhalb der breiteren Risikomanagementstrategie bewusst sind.

Beispielszenario: JK Enterprise

Um zu erklären, weshalb die heutigen Einzelprodukte Lücken lassen, nehmen wir auf JK Enterprise Bezug – ein fiktives Konsortium aus dem Gesundheitswesen. Wir stellen eine Entbindungsschwester und einen Notaufnahmepfleger in den Mittelpunkt.

Zugriffszertifizierung

Zugriffszertifizierungsprodukte sind unvollständig, wenn sie den Zugriff nur als Konto auf einem Server oder als Gruppenzugehörigkeit in einer Anwendung definieren, ohne dass bekannt ist, ob die lokale Richtlinie für die Zugriffssteuerung bezüglich Server oder Anwendung korrekt konfiguriert oder umgesetzt wurde.

Die Analyse und Überprüfung dessen, wer auf welche Ressourcen zugreifen kann, beginnt üblicherweise mit einem Datenabgleich, der die Benutzer mit den vorhandenen IT-Zugängen verknüpft. Der Benutzerzugriff auf IT-Ressourcen muss analysiert werden, damit über dessen Aufrechterhaltung entschieden werden kann. Auf dieser Basis etablieren Zertifizierungsregeln einen regelmäßigen Überprüfungsprozess und sorgen dafür, dass der Zugriff weiterhin den Vorschriften entspricht.

Produkte zur Zugriffszertifizierung erzielen einen Großteil ihres Nutzens bei der Zugriffsbereinigung, die im Zuge des anfänglichen Datenabgleichs durchgeführt wird, sowie bei der fortlaufenden Erfassung der Zertifizierungsdaten, die für Prüfung und Compliance herangezogen werden. Die Zertifizierung ermöglicht die Einführung einer fortlaufenden Prüfung von Benutzern, Rollen und zugeordneten Berechtigungen. Damit wird zwar den IAM-Governance-Anforderungen 1 – 3 Genüge getan, doch sind Zugriffszertifizierungsprodukte unvollständig, wenn sie den Zugriff nur als Konto auf einem Server oder als Gruppenzugehörigkeit in einer Anwendung definieren, aber die lokale Richtlinie für die Zugriffssteuerung bezüglich Server oder Anwendung nicht korrekt konfigurieren oder umsetzen.

So sind bei JK Enterprise Patienteninformationen in der Anwendung für Einweisung, Entlassung und Verlegung (Admission, Discharge and Transfer, ADT) gespeichert; der Zugriff ist mit der Benutzerzugehörigkeit zu einer Gruppe in dieser Anwendung verknüpft, wobei die korrekte Verwaltung der lokalen Richtlinie für die Zugriffssteuerung vorausgesetzt wird. Wenn jedoch ein Notaufnahmepfleger der Gruppe der Notaufnahmepfleger in der ADT-Anwendung zugeordnet wird, werden keine Gültigkeitsprüfungen durchgeführt. Ist die lokale Richtlinie für die Zugriffssteuerung korrekt konfiguriert und umgesetzt worden? Falls der Benutzerzugriff ungültig ist, erfolgt ohne Benutzereinrichtung keine Korrektur. Im Gegensatz zur Benutzereinrichtung wird durch die Zugriffszertifizierung allein kein Benutzerzugriff gewährt oder verweigert; diese führt vielmehr eine Methode zur Bereinigung und Prüfung auf Gültigkeit des Benutzerzugriffs ein. Davon abgesehen kann die Zertifizierung des Benutzerzugriffs anhand von Berechtigungen mühsam sein. Falls diese ohne die Verwendung von Rollen angewendet werden, wirft die hohe Anzahl der Berechtigungen ein administratives Problem auf. Die Anzahl der Rollen in einem Unternehmen sollte erheblich kleiner sein als seine Berechtigungen.

Aufteilung von Aufgabenbereichen

Was die Verwaltung von Zugriffskonflikten innerhalb eines Unternehmens betrifft, können wir einen Sachbearbeiter in einer Finanzabteilung als Beispiel nehmen, der dafür zuständig ist, neue Krankenhauszulieferer einzurichten und die zugehörigen Zahlungen zu genehmigen. Die Aufteilung von Aufgabenbereichen dient der Definition und Durchsetzung von Richtlinien bei Konflikten auf der Ebene der Rolle sowie der Berechtigung. So kann bei JK Enterprise ein Kreditorenbearbeiter nicht zugleich die Rolle eines Debitorenbearbeiters innehaben. Dies trifft auch auf die Berechtigungsebene zu: Ein Debitorenbearbeiter kann nicht zugleich die Funktion eines Prüfers innerhalb des ERP-Systems (Enterprise-Resource-Planning) ausüben.

Um Konflikte so effektiv wie möglich zu vermeiden, sollte ein Unternehmen zwei Verfahren kombinieren:

- *Präventive Aufteilung von Aufgabenbereichen, wenn die Richtlinie die Gewährung überlappender Zuständigkeiten verhindert, die einen potenziellen Konflikt für das Unternehmen darstellen*
- *Nachträgliche Aufteilung von Aufgabenbereichen, Analyse im Hinblick auf bereits vorhandene Konflikte*

Eigenständige Produkte zur Aufteilung von Aufgabenbereichen mögen zwar leistungsfähige Richtlinieneinschränkungen auf Transaktionsebene liefern, sind jedoch unzureichend, da sie in erster Linie auf ERP-Anwendungsrollen ausgerichtet sind. Häufig ist Funktionalität zur Aufteilung von Aufgabenbereichen im Lieferumfang von Produkten zur Rollenverwaltung oder zur Benutzereinrichtung enthalten. Diese Produkte erfüllen zwar Anforderung [5] bezüglich der Identitätsregelung, doch sie bieten in der Regel lediglich Kontrollen auf der Ebene der Rolle und der Gruppe und setzen voraus, dass einer Gruppe zugeordnete Benutzer eine Berechtigung repräsentieren. Diese Voraussetzung trifft jedoch nicht immer zu. Besser ist die Strategie, die Aufteilung von Aufgabenbereichen am Geschäftskontext auszurichten. JK Enterprise beispielsweise zieht es bei Notaufnahmepflegern vor, denselben Patienten an Wochenenden, wenn Personalmangel herrscht, aufzunehmen und zu entlassen.

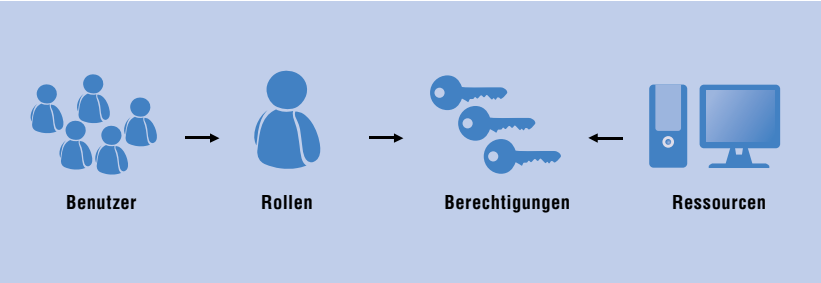

Abbildung 1: Rollenmanagement ermöglicht in einer Organisationsrollenstruktur, die den Benutzerzugriff auf Ressourcen regelt, Erkennung, Erstellung und laufendes Änderungsmanagement.

Rollenmanagement

Rollenmanagement ermöglicht in einer Organisationsrollenstruktur, die den Benutzerzugriff auf Ressourcen regelt, Erkennung, Erstellung und laufendes Änderungsmanagement, aber es gewährt oder verweigert keinen Benutzerzugriff. Es baut eine Rollenstruktur und einen Prozess auf, um folgende Bereiche effizienter zu verwalten:

- *Rollen, die eine Gruppe von Benutzern repräsentieren – häufig durch Aufgabenbereiche und Zuständigkeiten beschrieben – und deren Berechtigungen.*
- *Benutzergruppen, häufig als Geschäfts- oder Organisationsrollen bezeichnet (etwa Arzt, Labortechniker usw.); sie geben an, was ein Benutzer in seinem Job tut.*
- *Berechtigungsgruppen, auch als Anwendungs- oder IT-Rollen bezeichnet, zu einer Gruppe vereinigt, wenn sie eine spezielle Funktion innerhalb einer Anwendung ausüben (z. B. „Aktualisierung einer Krankenakte"). Geschäfts- und Anwendungsrollen regeln gemeinsam den für eine bestimmte Tätigkeit erforderlichen Zugriff.*

Anders als die Zugriffszertifizierung fügt das Rollenmanagement eine Abstraktionsebene hinzu, die die Zahl der Objekte zur Verwaltung des Benutzerressourcenzugriffs verringert und somit die Automation optimiert. Durch Kombination mit der Benutzereinrichtung kann die Korrektur automatisiert werden.

Unternehmen, die nach einer Rollenmanagementlösung suchen, pflegen folgende Maßnahmen zu ergreifen:

- *Erstellung von Rollendefinitionen und -struktur durch eine Analyse der Geschäftsziele, der Geschäftsprozesse und des Benutzerzugriffs*
- *Aufbau von Workflows zur Genehmigung und erneuten Zertifizierung, um das operative Änderungsmanagement hinsichtlich der Frage zu regeln, ob die Rolle noch definitionsgemäß angewendet wird*
- *Zuweisung der Rollenzugehörigkeit, die festlegt, wer für die definierten Rollen berechtigt ist*
- *Einrichtung von Workflows, um die Rollenzugehörigkeit auf konsistente Weise neu zu überprüfen*
- *Implementierung einer Rollenstruktur und deren Integration in eine Benutzereinrichtungslösung*
- *Kontinuierliche Überwachung, um die Compliance-Anforderungen in Bezug auf Prüfung und Berichterstellung zu erfüllen (und um potenzielle Rückmeldungen bereitzustellen, damit die Rollenstruktur im Hinblick auf eine ordnungsgemäße Zuordnung zwischen IT und Geschäftsbereich aktualisiert werden kann)*

Verbreitete Probleme des Rollenmanagements

Compliance, Sicherheit und Automatisierung sind die wichtigsten Triebkräfte hinter einer Rollenmanagementlösung. Wenn Rollenmanagementprojekte jedoch zu sehr auf die Technik ausgerichtet sind, können sie scheitern. Der Erfolg setzt ständige Kooperation mit dem Geschäftsbereich voraus, damit die Geschäftsrollen und -prozesse angemessen in die Anwendungsrollen integriert sind. Rollenbasierte Zugriffssteuerung ist nützlich, doch ein richtlinien- und kontextgesteuerter Ansatz ist notwendig.

Elemente des Kontextes:

- *Identitätskontext (z. B. Standort und Abteilungsbezeichnung)*
- *Servicekontext (z. B. Datenklassifizierung und Servicestandort)*
- *Umgebungskontext (z. B. Intranetanfrage und Tageszeit)*

Die Zugriffskontrollen müssen sich auf die gesamte Struktur von IT und Rechenzentrum erstrecken und zugleich einen breiteren Ansatz für das Unternehmensrisikomanagement einbeziehen.

Viele Rollenmanagementprodukte sorgen für beträchtlichen Mehrwert in den Bereichen Modellierung und operatives Management. Vielleicht erfüllen sie teilweise die Governance-Anforderungen 1 – 5 bezüglich der Clientidentität, doch gilt dies nicht für die zugrunde liegenden Identitätszuordnungen – durch Rollen – zu Anwendungen und Daten, die die Art und Weise der Governanceverwaltung festlegen.

Rollenmanagementprodukte setzen die IT- oder Anwendungsrollen häufig mit der Benutzerzugehörigkeit zu einer Gruppe in einer Anwendung gleich. Wie bereits im Abschnitt „Zugriffszertifizierung“ dargelegt, wird bei Richtlinien für die Zugriffssteuerung lokaler Anwendungen vorausgesetzt, dass sie ordnungsgemäß konfiguriert sind, um eine Berechtigung sicherzustellen. Doch die Aussage „ein Notaufnahmepfleger kann Patientendaten lesen“ sollte besser so ausgedrückt werden: „ein Notaufnahmepfleger kann vertrauliche Patientendaten innerhalb des Unternehmensnetzwerks lesen“. Die zweite Aussage liefert einen differenzierten Geschäftskontext sowie Metadatenmarkierungen. Der Ausdruck „innerhalb des Unternehmensnetzes“ zeigt die Definition und Durchsetzung einer Richtlinie an, die festlegt, wo ein Benutzer auf die Anwendung zugreifen kann, die Patientendaten enthält. Und „vertraulich“ ist ein Metadatentag, das die Klassifizierung sensibler Daten beschreibt. Wenn die Richtlinie Personen, Anwendungen und Daten regelt, wird durchgängige Governance mit Zurechenbarkeit erreicht.

Rollenidentifizierung[5] ist ein wichtiger Schritt bei der Rollenmodellierung, doch ihr Nutzen wird häufig überschätzt. Rollenmodellierung setzt eine erhebliche Kooperation zwischen Geschäftsbereich und IT voraus. Rollenidentifizierung ohne Kooperation hat nur begrenzten Nutzen. Der Nutzen ist in der anfänglichen Organisationsrollenstruktur am größten und in einer Produktionsumgebung geringer.

Darüber hinaus sind die Geschäftsprozesse, da Unternehmen innerhalb von Lieferketten zusammenarbeiten, stärker mit denen der Partner verzahnt. Demzufolge müssen die Kontrollen auf die Ebene der Daten und der Informationen angewendet werden – nicht nur auf die Ebene des Systems oder der Prozesse. Der Zugriff auf Informationen erfolgt immer mehr unternehmensübergreifend, was zu einer Dezentralisierung des Sicherheitsinformationsmanagements und zu dynamischen Beziehungen zwischen Partnern führt. Es besteht ein entscheidender Bedarf an einer umfassenden Semantik, um angepasste, differenzierte Zugriffsrichtlinien wie ein dynamisches Niveau von Schutzparametern zu definieren (beispielsweise Berücksichtigung der Bedrohungsstufe, vorliegende Transaktion und definierte Teams).

Die vorherrschenden Formen des Zugriffsmanagements, etwa eignerdefinierte Zugriffssteuerung (Discretionary Access Control, DAC), obligatorische Zugriffssteuerung (Mandatory Access Control, MAC) und rollenbasierte Zugriffssteuerung (Role-based Access Control, RBAC), sind statisch und werden diesen Anforderungen nicht gerecht. Beispielsweise eignet sich das RBAC-Verfahren, das sich üblicherweise auf zentralisierte Verwaltung von Benutzer-zu-Rolle- und Berechtigung-zu-Rolle-Zuweisungen verlässt, nicht gut für eine hochgradig verteilte Umgebung, da die Verwaltung auf Schwierigkeiten stößt, wenn Subjekt und Ressource verschiedenen Sicherheitsdomänen angehören.

Berechtigungsmanagement

Mit rollenbasiertem Zugriff auf wichtige Geschäftsanwendungen und Services stehen Unternehmen kritischen Anwendungssicherheitsrisiken gegenüber. Zunehmende Branchenverordnungen, Compliance-Anforderungen und Risiken hinsichtlich des Diebstahls von geistigem Eigentum machen es erforderlich, den Zugriff auf Anwendungen mittels rollen-, regel- und attributbasierter Berechtigungen zu kontrollieren. Eine auf Richtlinien basierende Berechtigungsmanagementlösung ermöglicht die zentrale Erfassung der Anwendungsrollen, das Verfassen und Verwalten der Berechtigungen und die Durchsetzung der adäquaten datenbezogenen Zugriffssteuerung. Ferner stellt sie einen „anwendungsorientierten" Ansatz für die traditionelle Aufgabe des Rollenmanagements dar und trägt dazu bei, die Anforderungen der betrieblichen Governance zu erfüllen.

Ein Beispiel: JK Enterprise möchte eine neue Call-Center-Anwendung für den Patienten- und Kundenservice einrichten und erstellt eine Anwendungsrolle „Patientendatenprüfer". Die mit dieser Anwendungsrolle definierten und verknüpften Regeln können Berechtigungen (etwa „Datensatz öffnen" oder „Datensatz anzeigen"), Zugriffskontrollen auf Datenebene (etwa „Zugriff auf persönlich identifizierbare Patientendaten beschränken") und zusätzliche Geschäftskontexte (etwa „Tageszeit" oder „Standort") enthalten.

Angesichts der Differenziertheit der Zugriffssteuerung kann es schwierig sein, das Berechtigungsmanagement für sich allein für das gesamte Unternehmen zu skalieren. Standards wie die Extended Access Control Markup Language (XACML) können diese Problematik mildern.

Privileged-Identity-Management

Privileged-Identity-Management regelt das erhöhte Risiko, das durch IT-Administratoren und Vorstandsmitglieder mit hohen Zugriffsebenen innerhalb einer Anwendung oder im gesamten Unternehmen entsteht. So kann zum Beispiel der Rootadministrator von JK Enterprise in der ADT-Anwendung auf sensible Patientendaten zugreifen. Ohne angemessene Kontrollen könnte er problemlos auf Patientendaten zugreifen und anschließend die Prüfprotokolle löschen, die den Zugriff aufgezeichnet haben. Unternehmen sollten getrennte Prozesse und Richtlinien für Benutzer-Life-Cycle-Management, Kennwortmanagement, Zugriffssteuerung und kontinuierliche Überwachung der Benutzeraktivität vorsehen, um diesem potenziellen Risiko gewachsen zu sein.

IBM verfolgt einen richtlinienbasierten Ansatz für die Verwaltung von Personen, Anwendungen und Daten

Unternehmen sollten einen ganzheitlichen Ansatz für IAM-Governance ins Auge fassen, der folgende Anforderungen erfüllt: Erkennung, Dokumentation und Analyse des Benutzerzugriffs; Einführung eines Prozesses zur Regelung des Benutzerzugriffs; Bewältigung von Geschäftskonflikten mithilfe von Einschränkungen; Durchsetzung von Richtlinien; kontinuierliche Überwachung. Ein richtlinienbasierter Ansatz für die Verwaltung von Personen, Anwendungen und Daten liefert die für IAM-Governance erforderliche Konsistenz und Flexibilität.

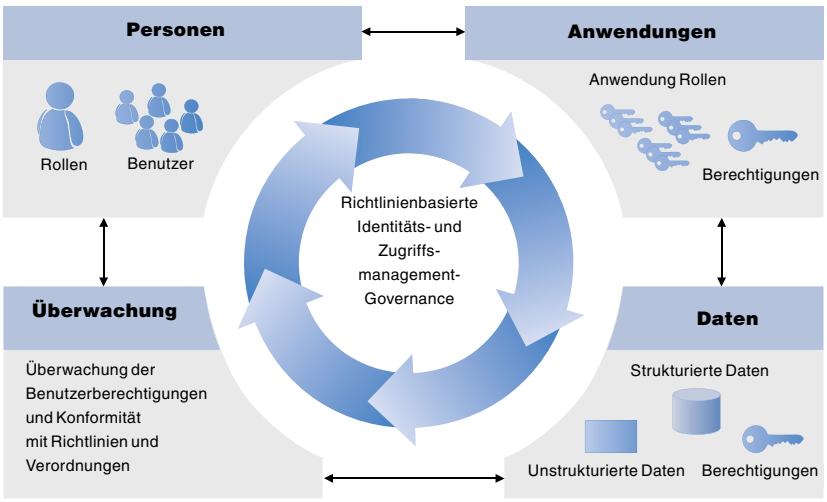

Abbildung 2: IBM verfolgt einen richtlinienbasierten Ansatz für IAM-Governance.

Ein richtlinienbasierter Ansatz für die Verwaltung von Personen, Anwendungen und Daten liefert die für effektive IAM-Governance erforderliche Konsistenz und Flexibilität.

Personen, Identitätsattribute und zugeordnete Rollen bilden kritische Verknüpfungen zwischen dem Geschäftsbereich und den Prozessen, die im Unternehmen für Transparenz, Zurechenbarkeit und höhere Effizienz sorgen. Anwendungen und zugeordnete Rollen stellen wichtige Berechtigungsverknüpfungen zu den Benutzern dar, sodass diese im erforderlichen Umfang auf Systeme und Informationen zugreifen können. Daraus folgt:

- *Die Verwaltung von Anwendungs- und Datenberechtigungen sollte die Geschäftskontexte von Identitäten, Services und der jeweiligen Umgebung berücksichtigen.*
- *Strukturierte und unstrukturierte Daten müssen effektiv verwaltet werden, um die adäquate Governance des geistigen Eigentums, der Kundendaten usw. sicherzustellen.*
- *Kontinuierliche Überprüfungen der Benutzeraktivität kommen nicht nur der Konformität mit den Richtlinien und Verordnungen zugute, sondern ermöglichen den Unternehmen auch die Korrektur regelwidrigen Benutzerverhaltens.*

Damit dieser ganzheitliche Ansatz für IAM-Governance durchgeführt werden kann, sollten Unternehmen den in Abbildung 3 gezeigten Lebenszyklus in Betracht ziehen. Die Einführung von IAM-Governance erfordert keine spezielle Chronologie.

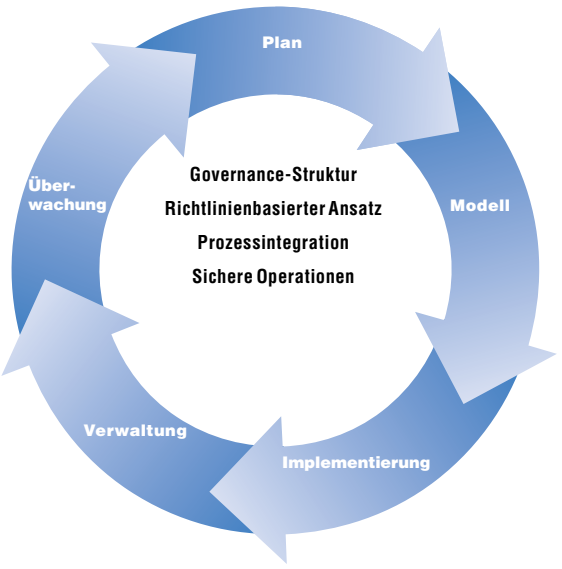

Abbildung 3: Ein durchführbarer IAM-Governance-Plan erfordert einen mehrstufigen, zyklischen Prozess.

Plan

Der erste Schritt bei IAM-Governance ist die Einrichtung vereinbarter Geschäftsziele und -prioritäten, einschließlich der Unterstützung einer konsistenten Übersicht. Anschließend sollte das Unternehmen eine Prüfung zur Erkennung der internen Prozesse und Daten durchführen – für alle Personen und Anwendungen und die gesamte Dateninfrastruktur – und diejenigen Prozesse untersuchen, die in dem Unternehmen oder der Abteilung den Benutzerzugang nach innen und nach außen ermöglichen. Welche Daten werden benötigt, um den Zugang zu ermitteln und bereitzustellen? Um eine Ausgangsbasis zu errichten, sollten die Unternehmen dokumentieren, wie die Geschäftsoperationen durchgeführt werden, und Richtlinien für Benutzerdaten und Zugriffsmanagement nutzen.

Die Erstellung von Geschäftsrollen sollte auf eine Abteilung oder einen Geschäftsbereich ausgerichtet sein. Ferner sollte die IT-Abteilung mittels einer Vergleichsanalyse zentraler Geschäftsprozesse mit führenden Mitarbeitern des Geschäftsbereichs kommunizieren, um zu demonstrieren, wie die aktuelle Organisationsrollenstruktur diese unterstützt. Daneben sollte die IT die Benutzer- und Berechtigungsdaten bereinigen, um bekannte Benutzer mit bekannten Konten und Berechtigungen abzugleichen. Diese Datenbereinigung umfasst die Identifizierung und Erfassung der relevanten Benutzer- und Berechtigungsdaten aus Zielsystemen wie Benutzereinrichtungslösungen, Microsoft® Active Directory®, Lightweight Directory Access Protocol (LDAP), ERP-Anwendungen und IBM Resource Access Control Facility (RACF).

Modell

Auf dieser Stufe sollte ein Unternehmen über die Basis an Anwendungsdaten und Vorgangs- und Geschäftsprozessinformationen verfügen, die es für die Modellierung und Entwicklung einer Rollenstruktur benötigt. Als guter Richtwert sollten 70-80 Prozent der Berechtigungen durch Rollen abgedeckt sein.

Unternehmen sollten ermitteln, wie sie mögliche Geschäftsrollen auf mögliche Anwendungsrollen abbilden möchten, und daraufhin die Daten für einheitliche Autorisierungssätze analysieren. Beispielsweise zeigt die ADT-Anwendung bei JK Enterprise, dass Notaufnahmepfleger normalerweise Patienten aus der Notaufnahme in eine andere Abteilung verlegen. Die Funktionen zur „Patientenverlegung" innerhalb der ADT-Anwendung sind ein Kandidat für eine Anwendungsrolle, die auf die Geschäftsrolle des Notaufnahmepflegers abgebildet wird.

Anwendungs- und Geschäftsrollen sollten getrennt sein, damit bei einer einzelnen technischen Änderung nicht die gesamte Rollenstruktur geändert werden muss. Rollendefinitionen können eine geschäftsrelevante Beschreibung dessen enthalten, wozu die Rolle eigentlich dient (z. B. kümmert sich eine Entbindungsschwester um neugeborene Babys) und wie sie mit der IT verknüpft ist (eine Entbindungsschwester kann Diagnosen für das Herzüberwachungssystem starten und ändern). Zuordnungen können über die Rollenhierarchie[6], über Richtlinien zur Aufteilung von Aufgabenbereichen, Zugriffszertifizierungsregeln und Benutzereinrichtungsregeln erfolgen. Die Einrichtung von Zugriffsrechten kann über Anwendungsrollen und XACML-Richtlinien zugewiesen werden, damit die Berechtigungen differenziert verwaltet werden können.

Notaufnahmepfleger bei JK Enterprise müssen bei der Verlegung eines Patienten die Patientendaten aktualisieren, doch das Krankenhaus respektiert die Privatsphäre des Patienten und definiert eine differenzierte, datenbezogene Berechtigungsrichtlinie. Die Regel legt fest, dass Notaufnahmepfleger vertrauliche Patientendaten nur an diesem Standort bearbeiten können und die Bearbeitung innerhalb des internen Unternehmensnetzwerks erfolgen muss. Diese Richtlinie regelt:

- *Informationskontext (vertrauliche Patientendaten)*
- *Identitätskontext (Pfleger und Patient befinden sich am selben Standort)*
- *Umgebungskontext (innerhalb des Unternehmensnetzwerks)*

Nach der Zuordnung beginnt die Rollenmodellierung. Die Modellierung sollte eine Simulation umfassen, damit das Unternehmen „Was wäre, wenn"-Szenarien zu sehen bekommt, die auf der vorgesehenen Rollenstruktur basieren. Die endgültige Struktur sollte sowohl vom Geschäftsbereich als auch von der IT-Abteilung genehmigt werden. Bei Berechtigungen, die nicht durch Rollen geregelt sind, sollte der Endbenutzer den Zugang über ein Self-Service-Portal anfordern. Die Workflows zur Genehmigung und erneuten Zertifizierung können mit dem Zugriffsanforderungsprozess verknüpft werden, um die Berechtigung nach der Genehmigung oder erneuten Zertifizierung zu erteilen oder zu widerrufen. Es ist von entscheidender Bedeutung, Workflow und Zugriffskorrektur im Voraus zu modellieren.

Entwurf und Modellierung der Richtlinien sollten die Überwachung der Benutzeraktivität vorsehen. So müssen Notaufnahmepfleger häufig rasch die Verordnung von Medikamenten übernehmen und haben keine Zeit, Genehmigungen einzuholen – ein riskantes Freigabekriterium. JK Enterprise nutztdie Überwachung der Benutzeraktivität, um zu bewerten, ob die dem Notaufnahmepfleger zugeordneten Anwendungsrollen konzeptionsgemäß eingesetzt werden. Dies ist ein wichtiger Rückmeldungskanal, da Unternehmen die Rollenstruktur überprüfen, um die Rollendefinitionen anzupassen.

Dieser Ansatz ermöglicht die Definition und Modellierung eines Prozesses, der den Benutzerzugriff für alle Personen, Anwendungen und Daten über ein mehrstufiges Richtlinienmanagement regelt. Darüber hinaus stellt er ein abstraktes Datenmodell bereit, das auf das Rollen- und Berechtigungsmanagement ausgerichtet ist, um verschiedene Berechtigungsdefinitionen zu verwalten.

Implementierung

Die Rollen- und Richtlinienzuweisung verknüpft die Benutzer mit Rollen und Richtlinien und kennzeichnet die Eigentümer der Rollen und Richtlinien. Der Schritt der Implementierung umfasst die Kontrollen rund um die Benutzerzuordnung sowie die Integration von Benutzereinrichtungslösungen, Anwendungen und Systemen.

Das Richtlinienmanagement wird ergänzt durch die Richtliniendurchsetzung, die aus gegenseitigen Kontrollen in den Geschäftsprozessen und aus der Durchsetzung in der Infrastruktur zur Laufzeit besteht. Die Richtliniendurchsetzung zur Laufzeit sollte detaillierte Methoden einbeziehen, sodass Zwischeninstanzen sowohl allgemeinen Zugriff als auch differenzierte Zugriffskontrollen auf Anwendungen und Daten durchsetzen können. Ein Ansatz auf der Basis einer serviceorientierten Architektur (SOA) unterstützt konsistentes Laufzeitmanagement sowie die Durchsetzung von Richtlinien und Identitäten für heterogene Systeme, Anwendungen und Daten, wobei Identität und Sicherheit als Services dargestellt sind. Auf diese Weise sind Durchsetzungs-, Entscheidungs- und Richtlinieninformationspunkte flexibel miteinander verbunden und können innerhalb und außerhalb des Unternehmens integriert werden.

Verwaltung

Wenn ein Unternehmen mit dem operativen Management beginnt, stellen Änderungsmanagementprozesse die ordnungsgemäße Änderungsgovernance für die Organisationsrollen- und Richtlinienstruktur sicher. Auf diese Weise können Unternehmen auch gewährleisten, dass für alle Compliance-Anforderungen ein System zur Erfassung der Prüfpunkte existiert.

Richtlinien zur Genehmigung und erneuten Zertifizierung dienen dem Änderungsmanagement auf der Ebene der Benutzer, der Rollen und der Berechtigungen; die Verwaltung wirkt sich kaum auf die Geschäftsabläufe aus. Wenn die Definition einer Geschäfts- oder Anwendungsrolle geändert werden muss, geschieht dies entweder proaktiv oder der Rolleneigentümer wird infolge der erneuten Zertifizierung gefragt, ob die Rollendefinition noch korrekt ist. Ist dies nicht der Fall, kann der Rolleneigentümer Schritte einleiten, um die für die Korrektur erforderlichen Änderungen zu delegieren und wieder zur Genehmigung vorzulegen. Die Durchsetzung der Berechtigungen ist ein entscheidender Punkt – es kommt nicht nur auf die Verknüpfung der Benutzer- oder Rollenzugehörigkeit mit einer Gruppe in einer Anwendung an, sondern auch auf die Durchsetzung vordefinierter Richtlinien zur Laufzeit.

Überwachung

Kontinuierliche Überwachung, Prüfung und Berichterstellung verschafft Unternehmen zwei wesentliche Vorteile. Erstens versetzen grundlegende IAM-Governance-Berichte, die differenzierte Berechtigungen hinreichend detailliert aufführen, Unternehmen in die Lage, die Prüfvorschriften seitens externer Verordnungen und unternehmensinterner Sicherheitsrichtlinien zu erfüllen.

Zweitens liefert die Prüfung und Überwachung der Benutzercompliance die Nagelprobe, was die Struktur der Organisationsrollen und Berechtigungen betrifft: Ist die Rollenstruktur daran ausgerichtet, wofür die Benutzer ihren Zugang einsetzen? Diese kritische Verknüpfung führt zu Rückmeldungen für Rollendefinitionen, Richtlinien und kontinuierliches Änderungsmanagement.

IBM IAM-Governance sorgt für die erforderliche Transparenz, Kontrolle und Automation, um geschäftsspezifische Benutzerzugriffsanforderungen mit höherer Zurechenbarkeit zu verwalten und die Regelung und Durchsetzung des Zugriffs sicherzustellen.

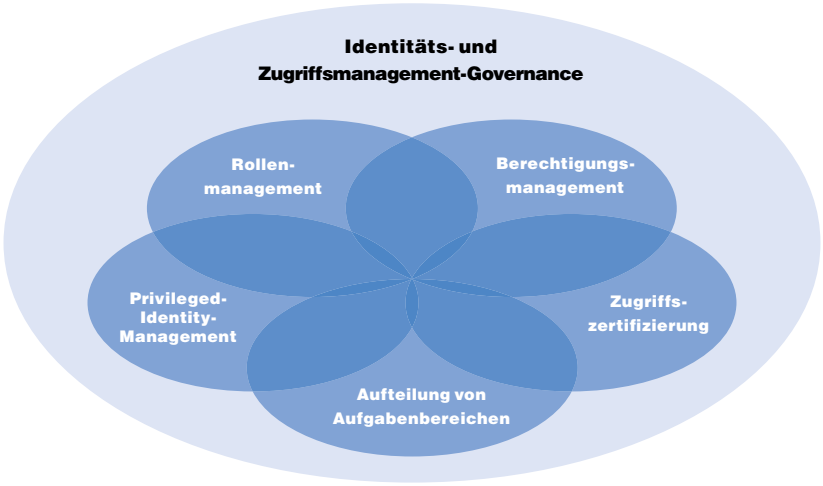

Abbildung 4: Auf der Basis ihrer Geschäftsprioritäten sollten Unternehmen mit einem Teilsegment des Identitätsmanagements beginnen, wie hier gezeigt, und anschließend einen Plan für vollständige IAM-Governance entwickeln.

IAM-Governance mit Zurechenbarkeit

Die derzeitigen IAM-Governance-Lösungen sind nützlich, aber unvollständig. Da Unternehmen bestrebt sind, den Benutzerzugriff auf Ressourcen zu verwalten, zu schützen und zu überwachen, sollten sie einen auf Richtlinien basierenden Ansatz in Betracht ziehen, um Personen, Anwendungen und Daten zu verwalten. IBM sorgt für die Transparenz, Kontrolle und Automatisierung, die für die Verwaltung geschäftsspezifischer Benutzerzugriffe mit höherer Zurechenbarkeit erforderlich sind. Auf der Basis ihrer Geschäftsprioritäten sollten Unternehmen mit einem Teilsegment des Identitätsmanagements beginnen (siehe Abbildung [4]) und anschließend einen Plan für eine vollständige IAM-Governance-Lösung entwickeln. Hier kann IBM helfen.

Weitere Informationen

Weitere Informationen zur Entwicklung einer ganzheitlichen IAM-Governance-Strategie erhalten Sie bei Ihrem IBM Ansprechpartner oder IBM Business Partner oder auf folgenden Websites:

- **ibm.com**/tivoli/products/identify-access-assurance
- **ibm.com**/tivoli/products/identity-mgr
- **ibm.com**/services/gbs
- **ibm.com**/services/us/index.wss/offering/iss/a1030826

Informationen zu IBM Service Management

IBM Service Management-Lösungen unterstützen Unternehmen bei der Verwaltung ihrer Geschäftsinfrastruktur und bei der Bereitstellung eines hochwertigen Service, der effektiv gesteuert wird und den Benutzern, Kunden und Partnern unterbrechungsfrei und sicher zur Verfügung steht. Unternehmen aller Größenordnungen können IBM Services, Software und Hardware für Planung, Ausführung und Management von Initiativen für Service- und Ressourcenmanagement, Sicherheit sowie Hochverfügbarkeit und Ausfallsicherheit von Geschäftsanwendungen und -prozessen nutzen. Flexible, modulare Angebote decken die Betriebssteuerung, die IT-Entwicklung, die Ressourcenverwaltung und die Systemverwaltung ab und basieren auf umfangreichen Erfahrungsberichten von Kunden, auf bewährten Verfahren und auf Technologien auf der Grundlage offener Standards. IBM agiert als strategischer Partner, um die Kunden bei der Implementierung der richtigen Lösungen zu unterstützen, die für schnellen Geschäftserfolg und ein schnelleres Unternehmenswachstum sorgen.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

[4] Zugriffsberechtigungen – Zugriff auf verschiedene IT- und physische Ressourcen (z. B. IT-Systeme und Gebäude), Geschäftsprozessressourcen (Geschäftsanwendungen) und Informationssysteme (Dateien, Datenbanken, Content-Management-Systeme und Dateifreigaben).

[5] Rollenidentifizierung – Prozess zur Analyse der Zielsysteme für einheitliche Berechtigungssätze, die gruppiert und zur Definition von Anwendungsrollen verwendet werden können.

[6] Rollenhierarchie – Vererbung zwischen Geschäftsrollen. Beispielsweise erbt ein Mitarbeiter von JK Enterprise, dem die Rolle des Krankenpflegers in der Notaufnahme zugewiesen ist, die allgemeinen Rollen von Krankenpflegern und fest Angestellten.

TIW14031-DEDE-00