Deloitte.

Access Governance @ Deloitte
Erfolgsfaktoren für eine unternehmensweite Strategie

Sicheres Zugriffsmanagement auf IT-Anwendungen ist und bleibt eine große Herausforderung für alle Unternehmen. Die Aufgabe ist bereits unter rein technischen und organisatorischen Gesichtspunkten äußerst komplex. Zusätzlich erschwert wird sie je nach Branche durch die Verpflichtung, regulatorische Anforderungen zu erfüllen. Umfassendes Zugriffsmanagement muss insofern organisatorisches Setup, verfügbare personelle Ressourcen, die mögliche technische Umsetzung und die branchenspezifischen Rahmenbedingungen berücksichtigen. Worauf sollten zukunftsorientierte Unternehmen bei der Erarbeitung einer nachhaltigen Access Governance-Strategie besonders achten?

Zugriffsmanagement eine reine IT-Aufgabe? Sicher nicht!

Historisch heißt in den meisten Unternehmen die Antwort auf die Frage, wer Zugriffsmanagement macht, zumeist: Die IT-Abteilung, die hat bei uns schon immer die Berechtigungen vergeben! Warum sollte man das ändern, wenn es doch scheinbar funktioniert hat?

Letztlich ist aber eben nicht die IT-Abteilung selbstständig für den Schutz unternehmenskritischer Daten und die Erfüllung der regulatorischen Anforderungen verantwortlich, sondern die Eigner der betroffenen Geschäftsprozesse oder das Management. Denn die IT-Abteilung dient der technischen Umsetzung und Bereitstellung der Zugriffsrechte, für deren Definition müssen aber die Fachabteilungen zuständig sein. Denn nur die Business Process Owner selbst sind fachlich überhaupt dazu in der Lage zu beurteilen, welchem Mitarbeiter in welchem Ausmaß Zugriff auf IT-Applikationen, auf Geschäftsprozesse und damit auf kritische Daten zu gewähren ist. Dies gilt umso mehr, wenn eine Unternehmung durch Expansion, M&A, neue IT-Systeme oder mobile Lösungen inhaltlich komplexer wird. Denn je komplexer das Unternehmen, desto anspruchsvoller wird auch ein integriertes Berechtigungsmanagement.

Zudem setzt sich bei den meisten Unternehmen das zwingende Selbstverständnis durch, die Verantwortung für Corporate Governance wahrzunehmen. Das Top-Management will insofern stärker und am besten in real time darüber informiert werden, welcher Mitarbeiter Zugriff auf unternehmenskritische Funktionen und Daten innerhalb der IT-Landschaft besitzt. Neben steigenden Anforderungen an ein flexibles Reporting und messbare KPIs treten Funktionstrennungen immer stärker in den Vordergrund. Diese werden nicht nur im Rahmen der Jahresabschlussprüfung gefordert. Vielmehr dienen diese zunächst dazu, kritische Geschäftsprozesse der Kontrolle durch die Verantwortlichen zu unterstellen und damit auch steuerbar zu machen.

Was ist eigentlich diese SoD?

Das Prinzip der Funktionstrennung oder Segregation of Duties (SoD) stellt sicher, dass ein einzelnes Individuum nicht zu weitreichende Gestaltungs- und Kontrollmöglichkeiten über einen Geschäftsprozess erlangt. Dadurch sollen einerseits unbeabsichtigte Fehler in der Ausübung der geschäftlichen Tätigkeiten vermieden und andererseits beabsichtigte betrügerische Handlungen erschwert werden. Konkret lässt sich das an einem Beispiel verdeutlichen: Wenn ein Mitarbeiter Lieferanten inklusive deren Bankverbindungen in einem ERP-System anlegen und gleichzeitig Zahlungen initiieren kann, so könnte er durch Zahlungsfreigaben an fiktive Lieferanten beträchtliche Finanzmittel unterschlagen.

Eine individuelle Berechtigungskonzeption für jede IT-Applikation?

IT-Applikationslandschaften wachsen historisch. Verbunden damit steigt auch die Komplexität des Berechtigungsmanagements. Erfahrungsgemäß zeigt sich, dass nicht selten in Firmen für jede IT-Applikation ein eigenes separates Berechtigungskonzept im Einsatz ist. Je nach Größe des Unternehmens werden Berechtigungsverwaltung und Administration zunehmend unbeherrschbar, treiben die involvierten Abteilungen an die Leistungsgrenze und können sogar im völligen Überblicks- und Kontrollverlust enden. Zusätzlich, und das ist beinahe noch bedenklicher, kann so nicht über verschiedene Systeme hinweg sichergestellt werden, dass die Anwender auch tatsächlich über ein konsistentes Zugriffsniveau verfügen. Geschäftsprozesse, die mehrere IT-Systeme betreffen, müssen einheitlichen Funktionstrennungsregeln und Daten, die in verschiedenen Business-Intelligence-Systemen zugleich gespeichert werden, müssen einem gleichartigen Schutz unterworfen sein.

Heterogene IT-Applikationslandschaft – homogene Access Governance

Sind die ersten Anstrengungen unternommen und die ersten Hürden auf dem Weg zu einem ausgereiften und passenden Berechtigungskonzept für ein ERP-System genommen, sollte das Schutzniveau auf weitere ERP-Systeme, IT-Applikationen oder sogar die gesamte IT-Landschaft implementiert werden. Separate und isolierte Berechtigungskonzepte maximieren den Aufwand und bieten gleichzeitig keine Möglichkeit, die geforderte bereichs- oder unternehmensweite Kontrolle auszuüben.

An dieser Stelle empfehlen sich holistische Identity & Access Management Lösungen. Die Identitäten der natürlichen Personen in einem Unternehmen oder einem Unternehmensverbund werden dabei an einer zentralen Stelle verwaltet, um jederzeit zu wissen, welcher User zu welchem Zeitpunkt Zugriffsrechte auf welche Systeme und damit Geschäftsprozesse besitzt. Ebenso werden IT-Applikationen zusammenhängend betrachtet, sodass Zugriffsrechte immer in Abhängigkeit von Geschäftsprozessen gewährt und kontrolliert werden. Erst dieser Ansatz ermöglicht eine Vereinheitlichung der Access Governance-Prozesse wie automatisierte(n) und funktionsgebundene(n) Vergabe und Entzug von Berechtigungen, regelmäßige Rezertifizierungen und einen ständigen Soll-Ist-Abgleich zwischen genehmigten und vergebenen Zugriffsrechten – und damit eine effiziente Unternehmenssteuerung aus Compliance- und Security-Gesichtspunkten.

Identity & Access Management-(IAM-)Lösungen

Kann man die folgenden Fragen überwiegend mit Ja beantworten, so ist mehr als empfehlenswert, sich über eine Identity & Access Management-Strategie ernsthafte Gedanken zu machen.

1) Besteht meine IT-Landschaft aus mehreren Systemen und Applikationen?
2) Müssen meine Mitarbeiter auf mehrere Systeme und Applikationen zugreifen, um ihre Aufgaben zu erfüllen?
3) Sind die Kosten der Nutzeradministration aufgrund der Komplexität vergleichsweise hoch?
4) Muss ich regulatorische Anforderungen für die Vergabe von kritischen Berechtigungen erfüllen?

Bringt man das Identity & Access Management (IAM) in den Kontext der oben beschriebenen Problematik der Administration und Handhabbarkeit der unterschiedlichen Berechtigungskonzeptionen, so kann man IAM als die strategische Weiterentwicklung der Einzelkonzeptionen bezeichnen. Jedoch bietet IAM weitaus mehr Möglichkeiten, Compliance-Anforderungen zu erfüllen, und kann bei richtigem Einsatz die Corporate Governance-Funktionen deutlich unterstützen.

Gerade in Zeiten der fortschreitenden Digitalisierung, der Nutzung von Cloud-basierten Services, von Bring-Your-Own-Device-(BYOD-)Strategien und der Nutzung von Mobile-Apps wird die herkömmliche Nutzer-und-Berechtigungs-Strategie auf den Prüfstand und vor schier unlösbare Herausforderungen gestellt.

Stehen Sie vor diesen Fragen und sind Sie auf der Suche nach passenden Lösungen? Deloitte ERS hilft Ihnen bei der erfolgreichen Durchführung von IAM-Projekten und begleitet Sie durch den gesamten Projektlebenszyklus.

Ihr Ansprechpartner

Alexander Huffer
Tel: +49 (0)30 2546 8409
ahuffer@deloitte.de

Für weitere Informationen besuchen Sie unsere Website www.deloitte.com/de

Stand 4/2016