

Identity Management und Governance für Sicherheit und Erfolg



Benutzer- und Zugriffsverwaltung ausgerichtet auf Geschäftsprozesse

Die Herausforderung

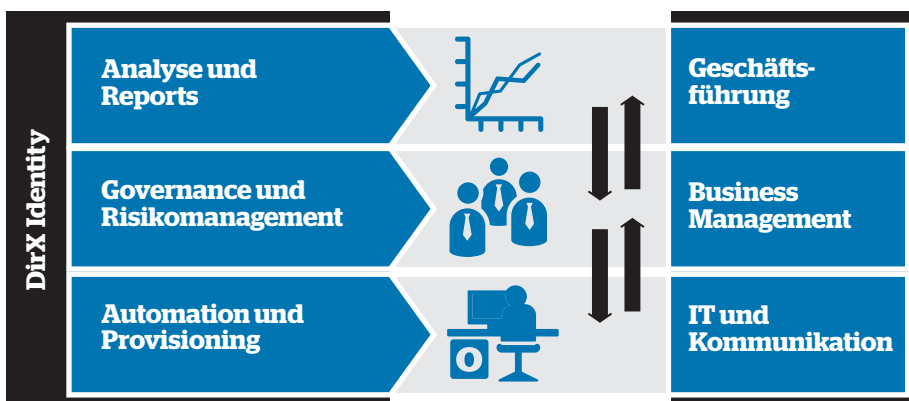
Geschäftsbeziehungen werden immer komplexer. Mehr und mehr Benutzer haben Zugriff auf IT-Systeme der Unternehmen. Der Druck ist permanent vorhanden, die Produktivität zu steigern und dazu jedem dieser Benutzer den Zugang zu ermöglichen, dabei aber gleichzeitig Datenschutz, Compliance und Kostenkontrolle sicherzustellen. Mit der Cloud, die weitere potentielle Sicherheitsrisiken erzeugt, verschärft sich diese herausfordernde Sicherheitssituation.

In dieser sich schnell verändernden Geschäftsumgebung ist ein wirksames Identity Management und Governance eine zwingende Notwendigkeit - sowohl für die Sicherheit des Unternehmens als auch für den Geschäftserfolg. Traditionell haben IT-Abteilungen Identity Management für die Effizienzsteigerung und Kostenreduktion eingesetzt. Jetzt werden Geschäftsbeziehungen und Compliance die Haupttriebfeder. Die Verwaltung und Sicherung von Geschäftsprozessen erfordern eine konsistente Administration der Benutzer, Rollen und Berechtigungen über alle Anwendungen und in den

Netzwerken der Geschäftspartner. Die Zuweisung der richtigen Zugriffsrechte zu den richtigen Ressourcen an die richtigen Benutzer zur richtigen Zeit ist unerlässlich zum Schutz der Unternehmensdaten und versetzt die Benutzer in die Lage, innovativ, produktiv, reaktionsfähig, regelkonform und kosteneffizient zu arbeiten.

Unsere Lösung

DirX Identity von Atos ist eine umfassende Lösung für die Herausforderungen heutiger Geschäftsumgebungen. Sie bringt IT-Management, Business Management und die Geschäftsführung mit dem Management der Benutzer und ihrer Zugriffsrechte in Einklang. Für die IT liefert DirX Identity das automatisierte User Provisioning; für das Business Management und das allgemeine Management bietet DirX Identity ein verbessertes Governance- und Risiko-Management, und für die Geschäftsführung stellt DirX Identity Analysefunktionen und Reports für die Steuerungs- und Kontrollaufgaben bereit. DirX Identity ist eine prozessgesteuerte, kundenspezifisch anpassbare, Cloud-fähige, skalierbare und hochverfügbare Identity Management und Governance Lösung, die Organisationen heute und in der Zukunft benötigen.



Die Treiber für Governance

Sicherheits- und Geschäftsaspekte sind wichtige Treiber für Identity und Access Management. Auch für eine starke Governance in diesem Bereich gibt es zwingende Faktoren.

Einhaltung von Vorschriften – Compliance

Die Absicherung von Benutzerzugriffen auf Unternehmensinformationen hat auch rechtlich an Bedeutung gewonnen. Weltweit verabschieden Regierungen Gesetze, mit denen die Sicherheit, Geheimhaltung und Integrität von schützenswerten Daten wie Benutzer und Finanzinformationen sichergestellt werden soll. Finanzdienstleister, Organisationen des Gesundheitswesens, Pharmazie-Unternehmen und andere Branchen benötigen eine sichere Infrastruktur für die Zugriffskontrolle. Wenn die gesetzlichen Anforderungen nicht erfüllt sind, kann dies rechtliche Konsequenzen haben, bis hin zu Gerichtsverfahren und hohen Geldstrafen. Um die Erfüllung der gesetzlichen Anforderungen zu belegen, müssen die Unternehmen nachweisen können, „wer wann was mit welcher Information gemacht hat“. Dies erfordert eine einheitliche Sicht auf die Zugriffsrechte des Benutzers für alle IT-Systeme, eine Möglichkeit, diese Zugriffsrechte kontinuierlich und automatisch durch identitätsbasiertes Audit und Berechtigungsprüfung nachzuverfolgen und eine Möglichkeit, diese Informationen langfristig zu archivieren und auszuwerten.

Verbreitung des eBusiness

Unternehmen stellen ihren Mitarbeitern, Abonnenten, Kunden und Geschäftspartnern Inhalte und Geschäftsprozesse über Portale und Online-Dienste zur Verfügung. Das eBusiness stellt Herausforderungen in Bezug auf Sicherheits-Governance, das Risikomanagement, Rechenschaftspflichten und den Nachweis der Einhaltung von Vorschriften. Wo Dienste von Cloud Service Providern bereitgestellt werden, sind weitere Aspekte zu beachten.

Organisationen müssen ihre Sicherheits-Policies klar definieren und konsistent über alle Systeme ihrer IT-Infrastruktur durchsetzen. Dazu müssen sie wissen, „wer die Berechtigung hat, auf welche Informationen wie zuzugreifen“.

Schnelle und flexible Verwaltung von Änderungen

Um die Produktivität zu maximieren und sich gegen Sicherheitsrisiken zu schützen, müssen neue Benutzer sowie Benutzer, die ihre Aufgaben wechseln, schnellstmöglich die zur Ausübung ihrer Tätigkeiten nötigen Zugriffsrechte bekommen. Um Sicherheitslücken zu schließen, müssen ausscheidenden Benutzern die Zugriffsrechte

so rasch als möglich wieder entzogen werden. Die Governance bezüglich der Benutzer und ihrer Zugriffsrechte muss konsistent und wirksam über die Benutzerlandschaft bleiben.

Kostenkontrolle

Um wettbewerbsfähig zu bleiben, müssen Kosten kontrolliert und reduziert werden. IT ist ein Schwerpunkt des Kostenmanagements, insbesondere bei steigenden Benutzerzahlen. Unternehmen wollen die Anzahl der Anrufe bei Helpdesks und Hotlines reduzieren, zum Beispiel für vergessene Passwörter. Sie wollen die administrativen Kosten verringern, die mit der Benutzerverwaltung und dem Provisioning verbunden sind.

Die Lösung

Eines der wesentlichen Hindernisse für Identity und Access Management sowie Governance, ist die Art und Weise wie IT normalerweise organisiert ist. Oftmals werden die Benutzerverwaltung, die Zugriffsverwaltung, das Passwortmanagement und das Audit pro System ausgeführt. Die IT-Administratoren verwalten die Benutzer und ihre Zugriffsrechte in jedem einzelnen IT-System des Netzwerks oder in der Cloud, üblicherweise manuell.

Die Benutzer bekommen eine Benutzerkennung (Account) und ein Passwort für jedes System, das sie benutzen. Jedes IT-System hat seine eigenen Audit- und Monitor-Funktionen, um die Änderungen der Benutzer und ihrer Zugriffsrechte in dem jeweiligen System zu verfolgen.

Diese Struktur ist eine Herausforderung für eine gute Benutzer- und Zugriffsverwaltung:

- ▶ Benutzer- und Zugriffsdaten sind auf mehrere IT-Systeme dupliziert und werden so mit der Zeit inkonsistent, so dass es schwer wird, aktuelle und richtige Informationen zu finden und Benutzer zu deprovisionieren.
- ▶ Dezentrale Audit- und Monitor-Funktionen erschweren das Nachvollziehen von Änderungen der Benutzer und ihrer Zugriffsrechte. Es gibt keine Möglichkeit zu sagen, wie die Zugriffsrechte eines einzelnen Benutzers insgesamt aussehen, so dass ein Audit für gesetzliche Anforderungen erschwert wird.
- ▶ Ein Passwort pro IT-Applikation hat zur Folge, dass sich die Benutzer viele verschiedene Passwörter merken müssen, eines für jedes System, das

sie benutzen. Die große Zahl von Passwörtern führt zu mehr Anrufen bei Helpdesks und Hotlines, zu reduzierter Produktivität, wenn Benutzer auf das Zurücksetzen der Passwörter warten, und zu steigenden Administrationskosten.

- ▶ Manuelle Administration ist teuer und fehleranfällig und führt zu Verzögerungen beim Provisionieren und Deprovisionieren von Benutzern. Dies senkt die Produktivität, gefährdet die Sicherheit und Compliance und führt zu Dateninkonsistenzen.

Der Weg zu einem wirksamen Identity Management und Governance ist ein unternehmensweites, plattformübergreifendes Provisioning und Access Management System mit zentraler und automatisierter Benutzerverwaltung. Das System steuert sicher, wirksam und wirtschaftlich den Zugriff auf IT-Ressourcen basierend sowohl auf Geschäftsrollen der Benutzer als auch auf Geschäftsregeln und -prozessen. Das System richtet Identity Management und Governance an den Geschäftsprozessen aus. Administrative Routine-Aufgaben und Entscheidungen werden von den Administratoren auf die Benutzer und ihre Führungskräfte verlagert, so dass Entscheidungen von Personen getroffen werden, die am besten wissen, was die Benutzer wirklich benötigen.

DirX Identity

DirX liefert übergreifende Identity und Access Governance Funktionalität, die nahtlos mit automatisiertem Provisioning integriert ist. Die Funktionalität umfasst Life-Cycle-Management für Benutzer und Rollen, plattformübergreifendes und regelbasiertes Provisioning in Echtzeit, Web-basierte Self-Service-Funktionen für Benutzer, delegierte Administration, Antrags-Workflows, Berechtigungsprüfung, Passwortmanagement, Metadirectory sowie Audit- und Report-Funktionalität.

DirX Identity gibt den richtigen Personen den richtigen Zugriff zu den richtigen Ressourcen zur richtigen Zeit.

DirX Identity liefert

Benutzerverwaltung

Ein korrektes und aktuelles Benutzerverzeichnis und ermöglicht die Zuweisung von Berechtigungen.

Rollenverwaltung

Eine logische Schicht für die Modellierung und Verwaltung von Berechtigungen mit Unterstützung von Rollenhierarchien und granularen Berechtigungen.

Berechtigungsprüfung

Für die Verantwortlichen die Möglichkeit zu überprüfen und zu bestätigen, dass die Zuweisung von Berechtigungen an Benutzer die Compliance-Anforderungen erfüllt.

Benutzer Self-Service

Für Benutzer die Möglichkeit, ihre eigenen Daten und Passwörter zu verwalten, Rollen zu beantragen, den Status eigener Anträge zu überprüfen und Zugriffsrechte an andere Benutzer zu delegieren.

Delegierte Administration

Die Verantwortung zur Verwaltung bestimmter Benutzergruppen wird an ausgewählte Administratoren delegiert.

Verwaltung von Organisationsdaten (Business-Objekte)

Verwaltung von Objekten, die für Identity Management Prozesse relevant sind oder dazu Bezug haben, wie Organisationseinheiten, Standorte, Kostenstellen und Projekte.

Antrags-Workflows

Die Möglichkeit, die Zuweisung von Berechtigungen, Anlage und Ändern von Benutzern und Rollen zu beantragen und in mehrstufigen Workflows zu genehmigen sowie diese zu bestätigen.

Passwort-Management und -Synchronisation

Die Verwaltung von zentralen Passwort-Policies, das Zurücksetzen von Benutzer-Passwörtern durch Administratoren. Benutzer können Passwörter für mehrere Anwendungen verwalten.

Verwaltung von gemeinsam genutzten Accounts

Verwaltung und Steuerung, wie Benutzer auf gemeinsam genutzte, privilegierte Accounts zugreifen.

Policy Management

Die Verwaltung von Sicherheits- und administrativen Policies, zum Beispiel Provisioning Policies, um Rollen automatisch zuzuweisen oder zu entziehen.

Provisioning in Echtzeit

Die Einrichtung der Zielsystemspezifischen Zugriffsrechte, in die die Benutzer-Rollenzuordnung aufgelöst wird und die Verwaltung der Benutzer-Accounts und ihrer Berechtigungen in den Zielsystemen.

Metadirectory

Integrierte und synchronisierte Directories, Benutzerdatenbanken und andere Verzeichnisse, um konsolidierte und konsistente Daten bereitzustellen.

Domänenverwaltung

Verwaltung von Mandanten mit getrennten Administrations- und Datenbereichen.

Verwaltung von Zielsystemen

Integration von Anwendungen und Systemen als Datenquellen und als Zielsysteme für das Provisioning.

Identity Web Services

Web Service Schnittstellen zur Integration der Identity Management Funktionalität in Portale und Kundenanwendungen.

Compliance

Unterstützung von Risiko-Management, um die Verletzung von Sicherheitspolicies zu vermeiden oder zu steuern, zum Beispiel um Funktionstrennungen (Segregation of Duties) für Berechtigungen in und zwischen Zielsystemen durchzusetzen.

Audit und Monitoring

Nachverfolgung von administrativen Änderungen und Erzeugung von Reports, um Benutzer und ihre Berechtigungen zu sehen.

Ihr Nutzen

- ▶ Bietet effiziente, automatisierte Verwaltung von Benutzern und ihren Berechtigungen
- ▶ Beschleunigt das Einrichten von Benutzern
- ▶ Reduziert Komplexität und verwaltet Risiken
- ▶ Unterstützt Prozesse zum Risikomanagement und Compliance
- ▶ Unterstützt schnelle und leichte Anpassung von Identity Management Prozessen an Kundenanforderungen
- ▶ Ermöglicht die nahtlose Integration mit IT Service Management (ITSM)
- ▶ Ermöglicht die zentrale und konsistente Verwaltung von ERP- und IT-Systemen
- ▶ Unterstützt bei der Verwaltung heterogener Umgebungen und ermöglicht die Integration horizontaler und vertikaler Lösungen (PLM, Gesundheitswesen, Zugangskontrolle, Smartcards, Unified Communication)
- ▶ Stellt exzellente Möglichkeiten zur Datenverwaltung bereit, um Identitäten zu bereinigen, zu konsolidieren und aktuell zu halten
- ▶ Liefert unterbrechungsfreie Services für geschäftskritische Einsätze mittels Hochverfügbarkeits- und Skalierungsoptionen.

Benutzer- und Rollenverwaltung

- ▶ Verwaltung des Lebenszyklus von Benutzern und Rollen
- ▶ Funktionale und organisatorische Rollen
- ▶ Kontextbasierte Rollenzuweisung
- ▶ Rollenhierarchien / -vererbung
- ▶ Funktionstrennungen (Segregation of Duties).

Berechtigungsprüfung und Audit

- ▶ Regelmäßige Bestätigung von Rollenzuweisungen
- ▶ Verwaltung von Kampagnen zur Berechtigungsprüfung
 - ▶ Validierung und Abgleich mit Zielsystemen
 - ▶ Monitoring von Aktivitäten
 - ▶ Reports und Dashboard.

- ▶ Regel- und Eventbasierte Verarbeitung
- ▶ Antragsworkflows und Genehmigungen
- ▶ Zeitgesteuerte Verarbeitung von Änderungen
- ▶ Identity Web Services
- ▶ Integration mit IT Service Management.

- ▶ Datenverwaltung
- ▶ Integrations-Framework für kundenspezifische Konnektoren
- ▶ Konnektoren für Identitätsquellen
- ▶ Umfassende Integration mit SAP
- ▶ Echtzeit-Provisioning von Zielsystemen.

Workflows und Prozesse

Provisioning und Identitätsquellen

**DirX
Identity**

Über Atos und Bull

Atos SE (Societas Europaea) ist ein führender Anbieter von digitalen Services mit einem Pro-forma-Jahresumsatz von rund 11 Milliarden Euro im Jahr 2014 und 93.000 Mitarbeitern in 72 Ländern. Atos unterstützt Unternehmen weltweit mit Beratungsleistungen und Systemintegration, Managed Services & Business Process Outsourcing (BPO) sowie Cloud-, Big-Data- und Sicherheitslösungen. Hinzu kommen Services von der Tochtergesellschaft Worldline, dem europäischen Marktführer für Zahlungs- und Transaktionsdienste. Mit seiner umfassenden Technologie-Expertise und tiefgreifendem Branchenwissen arbeitet Atos mit Kunden in unterschiedlichen Marktsegmenten zusammen: Banken, Bildung, Chemie, Energie und Versorgung, Gesundheit, Handel, Medien und Verlage, Öffentlicher Sektor, Produktion, Telekommunikation, Transport und Logistik, Versicherungen und Verteidigung.

Die Atos Gruppe verbindet Unternehmensstrategie, Informationstechnologie und Prozesse miteinander und hilft Kunden so, ihr Geschäft nachhaltig weiterzuentwickeln. Der Konzern ist der weltweite IT-Partner der Olympischen und Paralympischen Spiele und an der Pariser Börse Euronext notiert. Atos firmiert unter Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy und Worldline.

Ansprechpartner für weitere Informationen: [visit www.atos.net](http://www.atos.net)

Bull, Atos Technologien für die digitale Transformation

Bull ist die Atos Marke für Technologieprodukte und Software und ist in über 50 Ländern weltweit vertreten. Mit einer umfassenden Expertise von mehr als 80 Jahren technologischer Innovation, 2.000 Patenten und einem starken R&D-Team von 700 Mitarbeitern, unterstützt von der Atos Scientific Community, bietet Bull Produkte und Value-Added-Software. Diese unterstützen Kunden bei der digitalen Transformation, insbesondere in den Bereichen Big Data und Cybersecurity.

Bull ist der europäische Marktführer für HPC, zu den Produkten gehören unter anderem der energieeffiziente Supercomputer bullx; bullion, einer der weltweit leistungsfähigsten x86-Server für Big-Data-Anwendungen; Evidian, die Software-Security-Lösung für Identity and Access Management; Trustway, das Hardware-Security-Modul, sowie Hoox, das hochsichere Smartphone. Bull ist eine Tochter von Atos.

Weitere Informationen erteilt, www.atos.net/identity

Weitere Informationen: security@atos.net

Alle Marken sind Eigentum der jeweiligen Inhaber. Atos, das Atos Logo, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Yunano, Zero Email, Zero Email Certified und The Zero Email Company sind eingetragene Marken der Atos Gruppe. Atos behält sich das Recht vor, dieses Dokument jederzeit ohne vorherige Ankündigung zu ändern. Einige, in diesem Dokument beschriebene Angebote bzw. Teilangebote sind eventuell nicht überall erhältlich. Bitte wenden Sie sich an Ihre Atos Niederlassung vor Ort, um weitere Informationen über die in Ihrem Land erhältlichen Angebote zu erhalten. Dieses Dokument stellt keine vertragliche Verpflichtung dar. Dezember 2015 © 2015 Atos



Diese Broschüre wurde auf Papier gedruckt, das zu 40 % aus Öko-zertifizierten Fasern aus nachhaltiger Waldbewirtschaftung und zu 60 % aus recycelten Fasern in Übereinstimmung mit aktuellen Umweltstandards (ISO 14001) stammt.