E-book

IdentityPROCESS+

Der ultimative Leitfaden zu Best Practice Prozessen im Bereich Identity Governance und Administration

Omada

Vorwort

Die meisten Organisationen setzen heute hybride IT-Umgebungen ein, die teils am Standort, teils in der Cloud lokalisiert sind. Dadurch ist weniger transparent, wer warum auf welche IT-Systeme und -Anwendungen zugreift. In diesem Zusammenhang hat sich Identity Governance & Administration (IGA) zu einem wichtigen Eckpfeiler verlässlicher IT-Sicherheit entwickelt. Sie gestattet Unternehmen, Prozesse zum Erst Managen, dann Kontrollieren und Auditieren des Zugriffs auf Daten zu implementieren – eine wichtige Voraussetzung zur Senkung von Sicherheitsrisiken.

Im Laufe der letzten 20 Jahre hat Omada durch zahlreiche IGA-Anwendungen in Weltkonzernen und vielen mittelständischen Unternehmen umfassendes Know-how aufgebaut. Omada genießt die Anerkennung führender Analysten und hat vom Gartner Magic Quadrant 2019 im Bereich Identity Governance & Administration das Prädikat „Leader" erhalten. Omadas Expertise fand Eingang in IdentityPROCESS+, das Best-Practices-Prozess-Framework, das die Prozessbereiche festlegt, die erforderlich sind, um eine erfolgreiche Identity-Management- und Access-Governance-Lösung zu entwerfen und zu implementieren. Wir verwenden in diesem Buch die Abkürzung „IGA". Diesen benutzt das führende Analysten-Unternehmen Gartner im „Magic Quadrant for IGA (Identity Governance and Administration) Report" und im „Critical Capabilities for IGA Report".

Unser Framework beinhaltet alle systemübergreifenden bei Identity-Management und Zugriffskontrolle benötiten Prozesse. Das Framework von IdentityPROCESS+ umfasst aber nicht nur Gartners IGA-Definition, sondern geht sogar noch darüber hinaus. Wir hätten das Ganze also eigentlich IMAG – „Identity Management and Access Governance" – nennen sollen. Aus Gründen der Einfachheit haben wir uns aber für „IGA" entschieden.

Dieses Buch möchte CIOs, Compliance Manager CISOs, Security Manager, IT-Manager und alle Personen mit direktem oder indirektem Interesse am Thema Cybersicherheit darüber informieren, wie die Umsetzung von IdentityPROCESS+ sie dabei unterstützt, erfolgreich eine IGA-Lösung einzuführen und zu betreiben, die die Vorteile bei Sicherheit, Compliance und Effizienz liefert, die ein Unternehmen braucht.

Inhalte des ersten Kapitels:

- Übersicht der Herausforderungen, denen Organisationen gegenüberstehen, wenn sie die Digitalisierung zur Steigerung ihrer Wettbewerbsfähigkeit nutzen wollen.
- Einführung in die verschiedenen Aspekte von IGA.
- Überblick möglicher Herausforderungen bei der Umsetzung von IGA-Projekten.
- Überblicksartige Zusammenfassung des Best-Practice-Process-Frameworks IdentityPROCESS+ mit Einführung in die sieben Prozessbereiche, aus denen es sich zusammensetzt.

Das erste Kapitel erläutert, wie die Implementierung von Best Practices Organisationen hilft, Identities und Zugangsrechte während der gesamten Zeit zu managen, die ein Mitarbeiter im Unternehmen verbringt. Das schafft Zuverlässigkeit bei Governance, Benutzer-Zugriffsverwaltung in hybriden Umgebungen, dem Alignment von Identity-Management mit dem Unternehmen und beim Schutz wichtiger digitaler Assets vor und nach Entdeckung potenzieller Verstöße.

Im zweiten Kapitel wird genauer auf die Prozessbereiche eingegangen, um das technische Verständnis der Abläufe zu steigern. Die Funktion jedes Einzelprozesses wird detailliert erklärt und dabei auch auf die Implementierung von Best Practices, Beteiligung zentraler Stakeholder und vor der Analyse zu stellende Fragen eingegangen. Außerdem werden wichtige Empfehlungen gegeben. Nach Lektüre dieses Buches verfügen IT-Sicherheits-Profis sowie an Sicherheit und Compliance interessierte Führungskräfte über ein solides Verständnis für die Nutzung des Best-Practices-Frameworks für erfolgreiche IGA-Projekte.

Dank

Das IdentityPROCESS+ Framework basiert auf den Erfahrungen aus Tausenden von Arbeitsstunden, die Consultants, Partner und Kunden von Omada durch kontinuierliches Entwickeln, Verfeinern und Anwenden von IGA-Prozessen gesammelt haben. Wir möchten allen Beteiligten für ihre Mitarbeit und ihr Feedback danken. Marktübergreifender, vertikaler Input aus Organisationen hat sich als höchst nützlich erwiesen, um aus IdentityPROCESS+ eine zuverlässige Basis zu entwickeln, auf die Organisationen zukünftige IGA-Anwendungen aufbauen können. Wir entwickeln dieses Standard-Branchen-Framework aktiv Hand in Hand mit dessen integrierten Prozessen und der OIS-Plattform weiter, die Best-Practice-IGA-Prozesse automatisiert.

Mehr erfahren

Um Näheres über die Implementierung der Prozesse von IdentityPROCESS+ in Ihrer Organisation zu erfahren, kontaktieren Sie Omada bitte unter info@omadaidentity.com

Copyright 2021 - Omada A/S

Inhalt

KAPITEL 1

4 Einführung - Der Weg zu IGA
8 Identity Governance and Administration – zentrale Aspekte
9 Vorteile nutzen
10 Umgehen von Stolpersteinen bei IGA-Projekten
11 Einführung in IdentityPROCESS+
12 IdentityPROCESS+ – Festlegen der Vision
16 Zusammenfassung

KAPITEL 2

17 **IGA Best Practices im Detail**
19 Identity Lifecycle Management Prozesse
20 Managen des Identity Lifecycle
21 Prozess Onboard Identity
24 Prozess Change Identity
26 Prozess Off-Board Identity
27 Implementieren von Best Practices beim Identity Lifecycle Management
30 Wichtige Empfehlungen für Best Practices

34 **Access Management Prozesse**
35 Prozess Beantragung von Zugriffsrechten
36 Prozess Auswertung und Genehmigung
38 Prozess Provisionierung
39 Implementierung von Best Practices bei der Zugriffsverwaltung
40 Wichtige Empfehlungen für Best Practices

43 **Prozessbereich Business Alignment**
44 Managen von Business Alignment
45 Prozess Rolle managen
46 Prozess Policy managen
48 Prozess Kontext managen
49 Implementieren von Best Practices im Business Alignment
51 Wichtige Empfehlungen für Best Practices

53 Prozessbereich Management von Sicherheitsvorfällen

54 Prozess Sperren bzw. Reaktivieren von Zugriffen

56 Implementieren von Best Practices beim Management von Sicherheitsvorfällen

57 Wichtige Empfehlungen für Best Practices

58 Prozessbereich Governance

59 Managen der Governance

60 Prozess Berichtserstellung

61 Prozess Durchführung von Rezertifizierungen

65 Prozess Soll-/Ist-Abgleich

66 Prozess System- und Datenspeicher-Klassifizierung

68 Prozess Funktionstrennung (SoD)

69 Implementieren von Best Practices im Bereich Governance

70 Wichtige Empfehlungen für Best Practices

72 Prozessbereich Administration

73 Prozess Management von Zielsystemen

75 Prozess Password Management

78 Implementierung von Best Practices in der Administration

79 Wichtige Empfehlungen für Best Practices

81 Prozessbereich Auditing

82 Prozess Audit Trail

83 Prozess Audit-Verlauf

84 Prozess Audit-Protokoll

85 Prozess Audit-Policies

86 Prozess Audit-Response

87 Implementierung von Auditing-Best-Practices

88 Wichtige Empfehlungen für Best Practices

90 IGA Best-Practice-Prozesse: Der nächste Schritt

93 IGA Glossar

Der Weg zu IGA

Organisationen aller Größen und Branchen setzen on-premises- und verstärkt Cloud-Technologien ein, um effizienter zu arbeiten und in den Märkten, in denen sie operieren, wettbewerbsfähig zu bleiben. Dabei sparen sie Kosten ein, steigern ihre Produktivität und minimieren die Time-to-Market ihrer Produkte. Die Digitalisierung bringt zwar einerseits enorme Vorteile, kann aber auch ungewollte Herausforderungen mit sich bringen. Diese lassen sich in drei Hauptbereiche einteilen:

MANGEL AN ADÄQUATEN SICHERHEITSVOR-KEHRUNGEN

Zur Vermeidung von Sicherheitsverstößen bemühen sich Organisationen intensiv, dass alle IT-Systeme – on-premises und in der Cloud – strikte Identity- und Zugriff -Sicherheitsanforderungen erfüllen.

NON-COMPLIANCE

Bei der Umsetzung von Identity- und Access-Governance-Prozessen und der Durchführung notwendiger Verfahren, die sicherstellen, dass alle IT-Systeme und -Services interne und externe Vorgaben erfüllen, stoßen Organisationen immer wieder auf Hindernisse.

EFFIZIENT BLEIBEN

Zur Herausforderung wird dabei immer wieder der Anspruch, übermäßigen Arbeitsaufwand zu vermeiden, da die IT das Unternehmenswachstum durch neue Mitarbeiter, M&A-Aktivitäten und das kontinuierliche Hinzukommen neuer Anforderungen und IT-Systeme im Portfolio begleitet und dadurch ohnehin sehr beschäftigt ist.

Werden diese Herausforderungen adäquat angegangen, nutzen Organisationen die Vorteile heutiger IT-Systeme und neuer Technologien und steigern dabei ohne Sicherheitseinbußen die eigene Effizienz und Wettbewerbsfähigkeit. Vor näheren Erläuterungen zu den Best Practices, die Organisationen helfen, Identitäten zu managen und den Zugriff so zu regeln, dass die genannten geschäftlichen Anforderungen erfüllt werden, werfen wir zunächst einen Blick auf die gängigen unternehmerischen Herausforderungen,um die sich ergebenden Anforderungen.

MANGEL AN ADÄQUATEN SICHERHEITSVORKEHRUNGEN

Sicherheitsverstöße haben weitreichende Folgen

Intern oder durch Angriffe von außen verursachte Sicherheitsverstöße sind für Organisationen nicht einfach nur unangenehm, sondern können die Unternehmenstätigkeit empfindlich beeinträchtigen. Ob nun von innen durch Mitarbeiter und Lieferanten oder von außen – Angriffe können unabsichtlich oder bewusst ausgelöst werden. Die Wirkung bleibt stets die gleiche: Produktivitätseinbußen, beschädigte Geschäftsdaten, beträchtliche Clean-Up-Kosten, Diebstahl geistigen Eigentums sowie Rufschädigung, die Vertrauensverluste bei Kunden oder Partnern nach sich ziehen. Darüber hinaus sind auch Geldbußen und Rechtsstreitigkeiten für die Nichtbeachtung nationaler oder internationaler Gesetze zu betrachten.

Infolgedessen wird IT-Sicherheit auch bei der Unternehmensführung zum Thema. Ohne entsprechende Unterstützung durch die Unternehmensführung riskieren Unternehmen, dass notwendige Maßnahmen ohne die erforderliche Aufmerksamkeit bzw. Finanzierung anlaufen oder nicht alle nötigen Sicherheitsvoraussetzungen erfüllen.

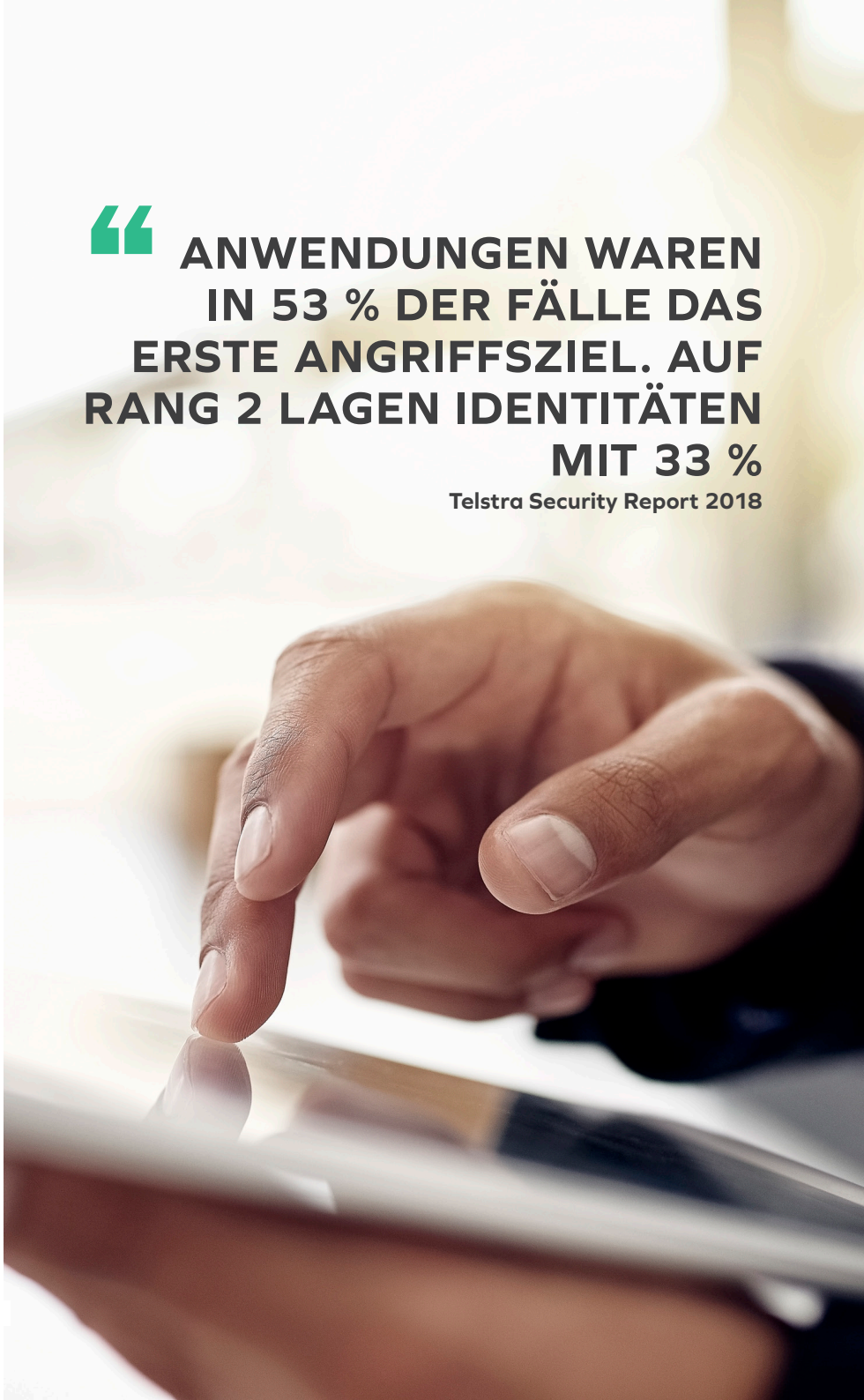
Sicherheit und die Steuerung von Identitäten und Zugriffsrechten

Organisationen werden sich verstärkt der Tatsache bewusst, dass das Durchsetzen geeigneter Prozesse zum Verwalten von Identitäten und dem Zugriff auf diese, ein Schlüsselelement zur Wahrung von Sicherheit ist – beispielsweise in Verbindung mit dem Verfahren zum korrekten, zeitnahen Entzug von Zugriffsrechten beim Auftreten eines Sicherheitsverstoßes.

Der Wert von Best-Practice-Standardprozessen

Durch Implementierung von Best-Practice-Standard-Prozessen für Identity Management und Access Governance stellen Organisationen sicher, dass sie alle Sicherheitsaspekte in Zusammenhang mit Identity Governance & Administration IT-Umgebungsübergreifend abdecken. Das Unternehmen erhält so die Gewissheit, dass Prozesse nach Best Practices abgedeckt und implementiert werden.

> **“ ANWENDUNGEN WAREN IN 53 % DER FÄLLE DAS ERSTE ANGRIFFSZIEL. AUF RANG 2 LAGEN IDENTITÄTEN MIT 33 %**
>
> **Telstra Security Report 2018**



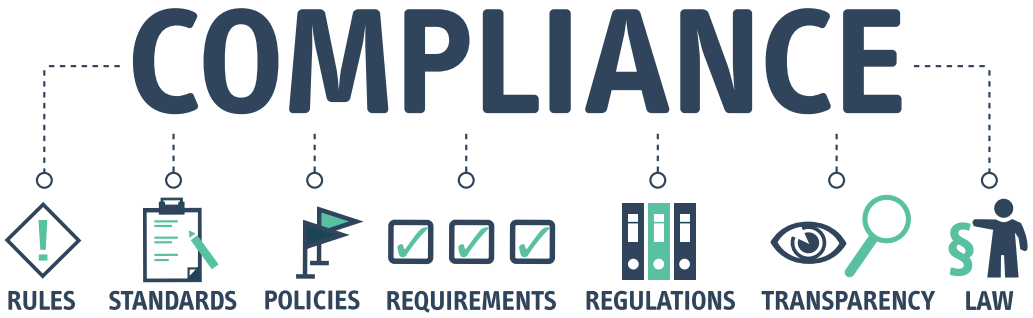
VORGEHEN BEI NON-COMPLIANCE

Die Einhaltung (Compliance) von Gesetzen und Bestimmungen ist geschäftskritisch

Über die Anforderungen im Bereich Cybersicherheit hinaus, messen die meisten Organisationen der Einhaltung eines weiteren, breiten Spektrums an Bestimmungen immer größere Bedeutung bei. Der Sarbanes-Oxley Act (SOX), Vorgaben der BaFin und die Datenschutz-Grundverordnung (DSGVO) betreffen alle Unternehmen mit europäischen Kunden. Auch der Australian Privacy Act und der California Consumer Privacy Act (CCPA) oder zahlreiche andere Gesetze und Bestimmungen wirken sich auf den Datenschutz aus. Deshalb müssen Organisationen sicherstellen, dass sie ihren entsprechenden Verpflichtungen nachkommen. Zu Compliance-Anforderungen gehören auch Kontrollmechanismen und das Protokollieren von Zugriffsgenehmigungen und -verläufen zu Auditzwecken. Für zahlreiche Unternehmen beispielsweise im Banken- und Finanzsektor ist der Nachweis der Einhaltung von Vorgaben essentielle Voraussetzung für die Betriebserlaubnis.

„Betriebserlaubnis" für Unternehmen

Im Geltungsbereich der DSGVO kommt die Erfüllung der Vorschriften mittlerweile für alle Organisationen einer „Betriebserlaubnis" gleich. Organisationen müssen unbedingt nachweisen können, dass Identities und deren Zugriff auf Daten dokumentierbar sind und nach Best Practices und hohen Sicherheitsstandards verarbeitet werden. Darüber hinaus versuchen viele Organisationen, ihren Kunden, Geschäftspartnern und zuständigen Behörden gegenüber den Nachweis zu führen, dass sie sich an bestimmte wie z. B. die durch ISO27001 o. ä. vorgegebene Sicherheitsregeln halten. Eine Nicht-Vorlage von Nachweisen über Regelerfüllung kann dazu führen, dass sowohl auf Kunden- wie auf Lieferantenseite Aufträge nicht erteilt werden, da es als riskant gilt, Geschäfte mit Unternehmen zu machen, die ihre Daten nicht adäquat verarbeiten.



Anders ausgedrückt: Es stellt mittlerweile einen Wettbewerbsvorteil dar, seinen Kunden und Geschäftspartnern versichern zu können, dass geeignete Maßnahmen ergriffen werden, um Daten zu schützen und hohe Sicherheitsstandards zu wahren.

Compliance und Zugriffssteuerung

Die Verwaltung von Identitäten und Zugriffsrechten hat im Zusammenhang mit der Wahrung der Vorgaben der DSGVO und zahlreicher anderer Gesetze und Vorgaben oberste Priorität. Die Fähigkeit zum Nachweis von Best-Practice-Prozessen ist von essentieller Bedeutung, da den Prüfern beim Audit nachzuweisen ist, dass eine Organisation die Kontrolle darüber hat, wer auf welche Daten zugreift. Wenn ein Unternehmen belegen kann, welche Regeln, Verfahren und Technologien vorliegen, um Zugriffsrechte zu steuern, Identitäten zu prüfen und bei evtl. Verstößen Meldung zu machen, steigt die Wahrscheinlichkeit, dass es die in diversen Regelwerken gemachten Vorgaben erfüllt.

Der Wert von Best-Practice-Standardprozessen

Durch Implementierung von Best-Practice-Standardprozessen können Unternehmen nachweisen, dass sie die erforderlichen Access-Governance-Prüfungen anwenden und so die Fragen von Auditoren rund um den Zugriff von Identitäten auf vertrauliche und sensible Daten wie z. B. Finanz- oder geschützte Daten zufriedenstellend beantworten.

EFFIZIENT BLEIBEN

Zentrales Element effizienter Betriebsabläufe

Wenn Organisationen wachsen und neue Systeme (sei es in der Cloud oder on-premises) einführen, größere Datenmengen verarbeiten, Mitarbeiter hinzukommen oder abwandern, an M&A-Aktivitäten teilnehmen oder ihr Geschäftspartner-Netzwerk erweitern, bedeutet das einen erheblichen Ressourcenaufwand. Sicherheitsmaßnahmen und Kontrollmechanismen müssen entsprechend effizient sein, um keinen Overhead zu produzieren.

Effizienz und Zugriffsverwaltung

Die Steuerung von Identitäten und deren Zugriffsrechten ermöglicht auch Kostensenkungen durch das Optimieren von Identity-Lifecycle-Prozessen wie z. B. Eintritt, Austritt sowie Wechsel von Mitarbeitern, Geschäftspartnern, Lieferant und Kunden in andere Abteilungen. Wenn Organisationen Prozesse zur Verwaltung von Identitäten und deren Zugriffsrechten festlegen, erreichen sie beträchtliche Zeiteinsparungen, da Prozesse wie Zugriffsprüfungen und -rezertifizierungen ebenso wie die Beantragung und Genehmigung von Zugriffsrechten vereinfacht wird.

Der Wert von Best-Practice-Standardprozessen

Die Implementierung von Best-Practice-Prozessen zur Verbesserung des Handlings von Usern, Identitäten, Zugriffsregeln, Rollen und Kontrollmechanismen stellt sicher, dass Unternehmen effizient vorgehen. Mitarbeiter, Manager und Eigentümer von Business-Systemen haben dadurch mehr Zeit für mehrwertgenerierende Tätigkeiten.

68 % ALLER UNTERNEHMEN VERZEICHNETEN IM LAUF DES VERGANGENEN JAHRES BEEINTRÄCHTIGUNGEN IHRER TÄTIGKEIT DURCH SICHERHEITSVERSTÖSSE

Telstra Security Report 2018

Das Wichtigste

Den richtigen Personen den richtigen Zugriff sichern
Sicherzustellen, dass Mitarbeiter, Lieferanten, Drittanbieter und Identitäten im Internet-of-Things (IoT) nur die Zugriffsrechte auf Systeme, Anwendungen und Daten erhalten, die sie brauchen, um ihre Aufgaben zu erfüllen und mit dem Unternehmen zu interagieren, ist für eine sichere, regelkonforme und effiziente Unternehmensführung von großer Bedeutung. Innerhalb der IT-Abteilung eines Unternehmens wird dieser Teilbereich als Identity Governance & Administration (IGA) bezeichnet.

IGA-Prozesse schaffen Compliance, Sicherheit und Effizienz
Eine IGA-Lösung ermöglicht der IT-Abteilung einer Organisation das Verwalten und Steuern sämtlicher Benutzerzugriffsrechte in einem hybriden IT-Umfeld von Enterprise-Systemen – on-premises oder in der Cloud.

IGA-Prozesse umfassen folgende Bereiche: Managen des bereichsübergreifenden Zugriffs auf Ressourcen im Rahmen des Identity Lifecycles innerhalb der hybriden IT von Organisationen (sei es für Anwendungen on-premises- oder in der Cloud), Audit- und Compliance-Reporting zur kontinuierlichen Sicherstellung von Risiko-Monitoring, Eintritt neuer Mitarbeiter, Durchführung von Access-Reviews und Rezertifizierungen quer durch alle Cloud- und on-premises- Anwendungen, ein strukturiertes Vorgehen beim Onboarding von Anwendungen sowie die Verwaltung von Zugriffsrechten für Anwendungen auf granularer Ebene im Einvernehmen mit den im Unternehmen geltenden Regeln sowie das Handling von Access-Assignment-Regeln und -Provisioning.

Unternehmen, die all diese Elemente effektiv verarbeiten können, sparen nicht nur Kosten durch Automatisierung, sondern sichern auch die Compliance und minimieren das Risiko von Datendiebstahl – sowohl intern als auch durch Hacker. Ein Schlüsselelement dieses Prozesses ist das Sicherstellen der Tatsache, dass Business-Systeme nur für diejenigen verfügbar sind, die den Zugriff zur Durchführung ihrer Aufgaben benötigen.

Unternehmen müssen IGA-Prozesse implementiert haben, um Sicherheit, Compliance und Effizienz zu gewährleisten und Organisationen vor Ereignissen zu schützen, die nicht nur den Ruf schädigen, sondern das Unternehmen schlimmstenfalls zur Geschäftsaufgabe zwingen könnten. In den oftmals cloudbasierten Umgebungen unserer Zeit mit ihren latenten Sicherheitsrisiken und strengen Gesetzesvorgaben wie der DSGVO, ist die Anwendung von Best-Practice-IGA-Prozessen eine Art „Betriebserlaubnis“ geworden.

Die Anwendung einer IGA-Lösung sollte als strategische Investition angesehen werden, die Organisationen hilft, unternehmensweit einen beträchtlichen Business Value zu realisieren.

Die Vorteile

nutzen

Die zentralen Prozesse von Identity Governance & Administration verschaffen Unternehmen erhebliche Vorteile.

SICHERHEIT

- **Image und Ruf des Unternehmens schützen**
  Das Vermeiden von Datenlecks durch Minimieren des Zugriffs auf sensible Daten und geschäftskritisches geistiges Eigentum sowie das Eingrenzen der Folgen von Sicherheitsverstößen durch Anwendung eines optimierten Prozesses zum Löschen betroffener Accounts bei Entdeckung von Sicherheitsverstößen.

- **Eigene Daten und geistiges Eigentum schützen**
  Erhalt eines 360-Grad-Überblicks über alle Identitäten und Zugriffsrechte bei allen Hybrid-Systemen und -Anwendungen sowie Prüfung der Frage, ob User sich im Einklang mit bestehenden Regeln und Vorgaben korrekten Zugriff verschaffen. Minimierung von Risiken, automatisches Erkennen verwaister bzw. inaktiver Accounts, die für Angriffe missbraucht werden könnten.

COMPLIANCE

- **Regelkonformes Vorgehen durchsetzen**
  Durchsetzen und Dokumentieren der Einhaltung von Zugriffsregeln über alle Anwendungen und Systeme hinweg. Zu den Regeln zählen u.a. Funktionstrennung (SoD), rollenbasierte Policies sowie Policies wie sie in SoX, HIPAA, CoBIT, DSGVO, ISO27001, von der BaFin, CCPA und anderen Regelwerken niedergelegt sind.

- **Schaffen von Zugriff zu Compliance-Prozessen**
  Einführen von Prozessen zum Umgang mit Sicherheitsverstößen durch kontinuierliches Monitoring des aktuellen Zugriffsstatus im Vergleich zum Soll-Status sowie ggf. Ergreifen von Gegenmaßnahmen.

EFFIZIENZ

- **Die Produktivität steigern**
  Rationalisierte Onboarding-Prozesse sparen Zeit, da Mitarbeiter und Externe vom ersten Tag an Zugriff auf die Systeme erhalten, die sie brauchen, um ihre Arbeit zu machen. Managen des Zugriffs, wenn Mitarbeiter die Rolle im Unternehmen wechseln sowie Widerruf des plattformübergreifenden Zugriffs, wenn dieser nicht mehr erforderlich ist.

- **Wertvolle Zeit nutzbar machen**
  Schaffen von beträchtlichen Zeiteinsparungen für Manager, interne Prüfer, System-Eigentümer Helpdesk- und andere Mitarbeiter durch Optimieren von Prozessen wie z. B. Access Reviews und Rezertifizierungsprozessen. Hieraus resultieren einsatzfertige Berichte für wiederkehrende Compliance-Audits.

Umgehen von Stolpersteinen

bei IGA-Projekten

IGA-Projekte können im Vergleich zu traditionelleren Projekten eine besondere Herausforderung darstellen, da ein solches Querschnittsthema sehr unterschiedlichen, auch widersprüchlichen, Anforderungen ausgesetzt ist und mit, Datenqualitätsthemen sowie unerprobten und fehlerbehafteten Prozessen zu rechnen ist. Zu beachten sind hierbei vor allem folgende Aspekte:

UNTERSCHÄTZEN DES AUFWANDS, UM ALLE STAKEHOLDER „AM BORD" ZU BEKOMMEN

Bei der Implementierung eines IGA-Projektes gibt es zahlreiche Stakeholder, u.a.:

- Den CISO und sein Sicherheitsteam, die für die Gesamtsicherheit der IT-Infrastruktur verantwortlich sind
- Eigentümer von Geschäftsanwendungen, die den Zugriff auf die von ihnen verwalteten Systeme kontrollieren möchten
- Compliance Officer und Schützer geistiger Eigentumsrechte, die sicherstellen müssen, dass der Zugriff auf geschäftskritische Systeme auf diejenigen beschränkt ist, die ihn benötigen
- Manager von Teams, die sicherstellen müssen, dass jedes Teammitglied zum richtigen Zeitpunkt Zugriff auf das richtige Informations-Level erhält
- Interne Auditoren, die einen transparenten Überblick über Zugriffsrechte benötigen
- Die IT, die sachgemäße Services für alle Stakeholder zu erbringen hat und selbst nicht unerhebliche Administrationsanforderungen hat

Unterschätzt man die Notwendigkeit, die verschiedenen Stakeholder in einer frühen Projektphase „an Bord" zu holen, kann das zu Verzögerungen und geringer Akzeptanz führen.

FOLGEN DER NICHT-ANWENDUNG VON BEST PRACTICES

Unternehmen, die an alten Verfahrensweisen festhalten, um den Status Quo nicht durcheinanderzubringen, könnten eines Tages vor ineffizienten Prozessen stehen, die Compliance-Anforderungen der Zukunft nicht erfüllen und nicht über die benötigte Reaktionsschnelligkeit verfügen. Aus Sicht von IGA-Systemen kann die Nicht-Anwendung von Best Practices zu unnötigen und (zu) komplexen Individualisierungen von Produkten führen.

ÜBERAMBITIONIERTE „BIG-BANG"-PROJEKTPLANUNG

Wer zu ambitioniert ans Werk geht und versucht, gleich in der ersten Phase alles umzusetzen – anstatt Werte früh und oft zu identifizieren und zu liefern –, muss damit rechnen, dass dies unnötig Ressourcen bindet und in der Organisation geringe Akzeptanz findet.

UNTERSCHÄTZEN DES AUFWANDS ZUR VERBESSERUNG DER DATENQUALITÄT

Daten über Mitarbeiter, Lieferanten, externe Geschäftspartner, Kunden und deren Zugriff werden oftmals in einer Vielzahl von Systemen wie z. B. verschiedenen Datenbanken und Tabellenblättern in unterschiedlichen, cloudbasierten und on-premises befindlichen Systemen gespeichert. Solche Daten – und dies umfasst auch Quellsysteme (HR-Daten) – sind oftmals in keinem für IGA passenden und gepflegten Zustand. Die Erfassung, Vereinheitlichung, Korrelierung und Verarbeitung dieser Daten kann technische, politische oder juristische Herausforderungen mit sich bringen und zeitaufwändig sein.

Unterschätzt man den Zeitaufwand zur Optimierung von Datenqualität (z. B. beim Einholen von Informationen bei Vorgesetzten zur Korrelierung von Benutzerkonten mit tatsächlichen Mitarbeiter- und Externen-IDs), kann dies zu beträchtlichen Projektverzögerungen führen.

IdentityPROCESS+

IdentityPROCESS+ ist ein umfassendes Best-Practice-Process-Framework, das die wichtigsten Prozesse beschreibt, die zur Sicherung eines erfolgreichen IGA-Einsatzes erforderlich sind. Diese Rahmenstruktur wurde mit dem Ziel entwickelt, erfolgreiche IGA-Projekte für Organisationen rund um die Welt zu unterstützen und soll Organisationen helfen, bewährte Best-Practice-Prozesse umzusetzen, ohne dass hierbei „das Rad neu erfunden" werden muss.

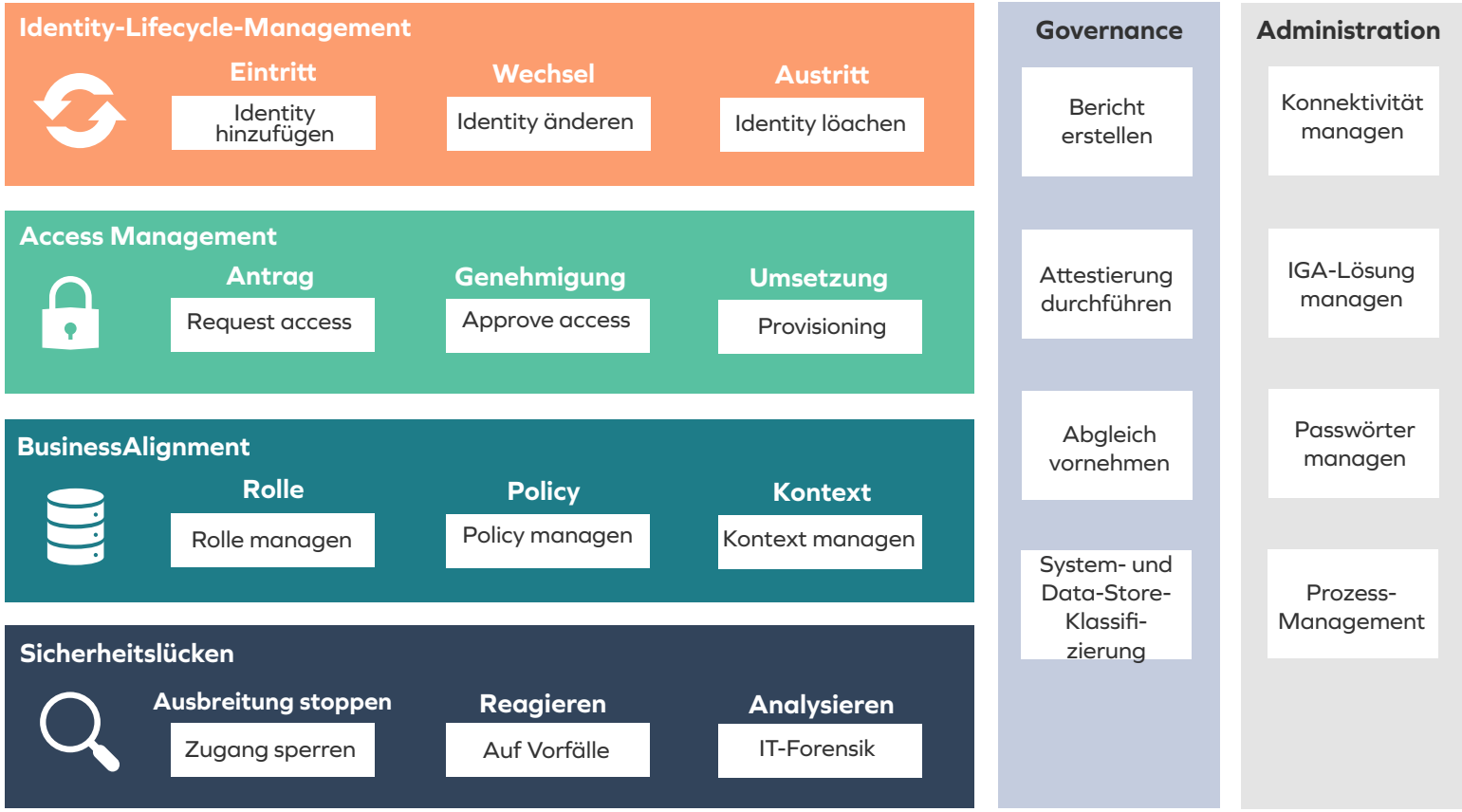


Abb. 1: Die Prozessbestandteile von IdentityPROCESS+

IdentityPROCESS+

Festlegen der Vision

Die Rahmenstruktur von IdentityPROCESS+ lässt Organisationen Ihre Vision von IGA-Projekten beschreiben und die geplanten Vorteile umzusetzen. Organisationen, die diese Struktur übernehmen, können ihre Chancen auf erfolgreiche IGA-Projekte deutlich steigern.

VERSCHIEDENE STAKEHOLDER, VERSCHIEDENE ANFORDERUNGEN

Um für ein IGA-Projekt einen Buy-in von jedem Stakeholder-Typ in der Organisation zu erwirken, muss man geschäftliche Vorteile quantifizieren und die damit verbundenen Geschäftsprozesse einschließlich der von ihnen geschaffenen Werte visualisieren. IdentityPROCESS+ hilft Organisationen schon in einem frühen Stadium beim Mapping geschäftlicher Vorteile auf Geschäftsprozesse – und hilft so, eine korrekte Ausrichtung zu sichern und Missverständnissen vorzubeugen.

Hier einige der Vorteile von IdentityPROCESS+:

- ✓ Leichte Anwendung von Best-Practice-Prozessen.
- ✓ Dokumentieren, dass Best-Practice-Identity- und zugriffsbezogene Kontrollmechanismen implementiert sind, um die Fragen von Auditoren rund um den Zugriff von Identitäten auf vertrauliche und sensible Daten wie Finanz- oder geschützte Daten zufriedenstellend zu beantworten.
- ✓ Anwendung von Best-Practice-Prozessen zum Optimieren des Handlings von Usern, Identitäten, Zugriffsregeln, Rollen und Kontrollmechanismen.
- ✓ Sicherstellen, dass eine Organisation alle Sicherheitsaspekte im Zusammenhang mit Identity Governance & Administration im Rahmen eines Projektes abdeckt, damit das Unternehmen sicher sein kann, dass Prozesse nach Best-Practice-Maßstäben abgedeckt und implementiert werden.
- ✓ Managen diverser Stakeholder durch Aufgliedern des gesamten IGA-Projektes in kleinere Phasen vereinfacht für das Projektteam die Visualisierung und den Nachweis der geschäftlichen Vorteile gegenüber anderen Abteilungen.
- ✓ Visualisierung der Geschäftsprozesse und erwarteten Ergebnisse schon in frühen Projektstadien, damit Stakeholder die Vorteile der Anwendung der Prozesse verstehen.
- ✓ Die Organisation so strukturieren, dass auch Benutzer, die keine Fachleute sind, leicht an dem Projekt mitwirken können.
- ✓ Vermeiden des Risikos überambitionierten Vorgehens durch Implementieren aller Inhalte gleich beim ersten Business Case – stattdessen identifizieren von Quick Wins bei früher und häufiger Wertgenerierung.
- ✓ Vermeiden komplexer Individualisierungen, falls / wenn eine IGA-Lösung implementiert wird, da die Best Practice bekannt ist.
- ✓ Validierung der Automatisierung von Lösungen anhand von Best Practices, die in Tausenden von Arbeitsstunden qualifizierter Profis entwickelt wurden.
- ✓ Herausnehmen der Spannungen, die eine neue, aber nicht richtig gemanagte IGA-Lösung erzeugen könnte.

IdentityPROCESS+ unterteilt die in einem IGA-Lösungspaket enthaltenen Prozesse in sieben Kern-Prozessbereiche auf, von denen jede einen Schlüsselbereich eines IGA-Gesamtpakets abdeckt. Jeder dieser Bereiche umfasst eine Reihe von Prozessen. Diese vordefinierten Prozesse decken alle wichtigen Prozesse ab, die von Organisationen beim Managen von Identitäten und bei der Durchführung von Access Governance zu implementieren sind

IDENTITY LIFECYCLE MANAGEMENT

Zentrales Element beim Managen von Identities ist das Joiner-Mover-Leaver-Konzept, das Mitarbeiter-Zugriffsrechte managt, wenn diese in das Unternehmen eintreten, die Abteilung bzw. Rolle wechseln oder wieder aus dem Unternehmen austreten. Die manuelle Bearbeitung solcher Änderung ist zeitraubend, kostenintensiv und fehleranfällig. Mögliche Folge: Ein Unternehmen kann unnötigen Risiken ausgesetzt sein, wenn Personen der Zugriff auf Systeme gewährt wird, zu denen sie keinen Zugriff haben sollten. Identity Lifecycle Management umfasst auch Prozesse, die eine Identität in jeder dieser Phasen managen.

Onboard Identity
Ein Unternehmen sollte unbedingt sicherstellen, dass der ursprüngliche Eintrittsprozess effizient gehandhabt wird, damit neue Mitarbeiter vom ersten Tag an produktiv sein können und Zugriff auf alle Systeme haben, die sie brauchen, um ihre Aufgaben zu erledigen. Ansonsten kann es sein, dass sie in den ersten Tagen ihrer neuen Tätigkeit darauf warten, Zugriff auf Systeme zu erhalten. Ein ähnlicher Prozess zum Onboarding von Lieferanten und Festlegen technischer Identitäten bzw. nicht-persönlicher Accounts wird auch im Rahmen von IdentityPROCESS+ definiert.

Änderungen der Identity
Im Laufe ihrer Tätigkeit in einem Unternehmen wechseln Mitarbeiter immer wieder die Rollen, werden befördert oder wechseln zu einer anderen Abteilung. Bei einer neuen Position benötigt man in der Regel zusätzlichen Zugriff auf bereits genutzte oder neue Systeme. Dann ist es nicht nur wichtig, diesen zu gewährleisten, sondern auch von entscheidender Bedeutung, sicherzustellen, dass alle Zugriffsrechte, die der betreffende Mitarbeiter nicht mehr benötigt, deaktiviert werden. Unterbleibt dies, erhält der Mitarbeiter im Laufe der Zeit immer umfangreichere Zugriffsrechte. Das könnte dazu führen, dass ein Benutzer Rechte hat, die Unternehmenspolicies wie der Funktionstrennung (SoD) zuwiderläuft. Damit steigt auch das Risiko von Datenmissbrauch, wenn der Account der Betreffenden gefährdet ist. Hat ein Benutzer nämlich Zugriff zu mehr Systemen als nötig, können Hacker sich dies für ihre Zwecke zunutze machen.

Off-board-Identity
Verlässt ein Mitarbeiter oder Lieferant das Unternehmen, muss deren Zugriff zu allen Business-Systemen und -Anwendungen deaktiviert werden, damit kein Einloggen in Unternehmenssysteme mehr möglich ist. Das korrekte Off-boarding der Identität eines scheidenden Mitarbeiters/Externen und die Erhaltung einer auditfähigen Historie ist ein wichtiger Schritt zur Absicherung Ihrer Organisation.

ACCESS MANAGEMENT

Zentraler Bestandteil der Verbesserung eines effizienten Identity Managements ist die Sicherstellung der Tatsache, dass Endbenutzer den Zugriff auf digitale Ressourcen so schnell und effizient wie möglich beantragen und Manager diesen ebenso schnell und effizient bewilligen können. Die Zugriffsverwaltungsprozesse innerhalb des IdentityPROCESS+ Framework erleichtert Endbenutzern den Zugriff zu Ressourcen wie z. B. gemeinsam genutzten Festplatten oder Geschäftsanwendungen. Der Workflow der Zugriffsverwaltung leitet die Anfrage an einen zuständigen Manager weiter, der dann den Zugriff genehmigt oder verweigert.

Beantragung von Rechten
Eine effiziente Zugriffsverwaltung verbessert die Produktivität von Mitarbeitern, da dieseneue Zugriffsrechte beantragen können, sobald eine geschäftliche Situation deutlich macht, dass sie zusätzlichen Zugriff benötigen, um ihre Pflichten auszuüben. Dieser Prozessbereich beschreibt Prozesse für Self-Service-Berechtigungsanträge, wodurch ineffiziente, arbeitsintensive manuelle Prozesse durch Vereinheitlichung von Antragsprozessen ersetzt werden.

Über die Genehmigung von Systemzugriffen hinaus werden auch Rezertifizierungen durchgeführt – ad hoc und in periodischen Abständen. Diese Prozesse stellen sicher, dass Mitarbeiter und Externe nach wie vor Zugriff auf bestimmte Ressourcen haben. Dies wiederum stellt sicher, dass Mitarbeiter und Externe keine umfassenderen Zugriffsrechte erhalten als nötig und verhindert, dass Externe noch Zugriff haben, wenn ihre Zusammenarbeit mit einem Unternehmen schon lange beendet ist (weitere Details, siehe Abschnitt „Governance“).

Approve accessZugriff genehmigen
Dieser Teil umfasst mehrere Prozesse für Workflows mit Single- und Multi-Level-Genehmigungen. Die Zugriffsverwaltungsprozesse umfassen ebenfalls das Terminieren von Benutzerberechtigungen entweder nach Eintreten eines Ablaufdatums oder bei Widerruf durch einen Manager bzw. Administrator.

Provisionierung
Diese Prozesse umfassen Prozesse zur automatisierten Provisionierung bzw. Deprovisionierung von Benutzerberechtigungen unter Anwendung von Policies gesteuerten Zugriffsregeln und von diesen definierten Rollen. Die automatisierte Provisionierung und Zuweisung von Zugriffsrechten über Regeln und Policies erleichtert den schnellen Roll-out des Zugriffs zu neuen Geschäftsanwendungen.

BUSINESS ALIGNMENT

Die Benutzer-Akzeptanz bei IGA-Systemen vertraut darauf, dass das System für das Unternehmen so benutzerfreundlich wie möglich ist. Um dies sicherzustellen, verwendet das IdentityPROCESS+ Framework Rollen, Kontexte

und Policies, die die Organisation präzise abbilden. Die Erstellung der richtigen, maßgeschneiderten Modelle für verschiedene Rollen, Zuweisungs- und Ausschlussregeln sowie die Verwaltung von Kontexten führt zu einer erheblichen Optimierung des IGA-Systems, welches Organisationen unterstützt, die erkannten ROI-Vorteile schon in frühen Projektphasen zu nutzen.

Rollen

Rollen beschreiben Rechtebündelungen für ähnliche Jobprofile. Beispiele für Rollen sind u.a. Verkaufsmitarbeiter, Buchhalter, Programmierer oder Projektmanager. Rollen dienen dazu, Benutzern bei Eintritt in ein Unternehmen oder dem Wechsel in eine andere Rolle gleichwertige Zugriffsrechte auf Business-Systeme zu gewähren.

Ohne Rollen müsste man sämtliche Zugriffsrechte für jeden User einzeln einrichten. In Organisationen mit zahlreichen Usern ist das manuelle, einzelne Zuweisen von Zugriffsrechten eine ressourcenintensive und fehleranfällige Aufgabe. Ein weiteres Problem: Die Bereitstellung von Zugriffsrechten durch einfaches Kopieren der Zugriffsrechte bereits vorhandener Benutzer. So kann es sein, dass einem neuen Mitarbeiter unbemerkt nicht die richtigen Rechte zugewiesen werden, da ein anderer Mitarbeiter mit ähnlicher Rolle aufgrund längerer Tätigkeit für das Unternehmen umfassendere Rechte hat. Rollen dienen auch dazu, die Einschränkung von Zugriffsrechten wie z. B. die Funktionstrennung (SoD) zu definieren. IdentityPROCESS+ definiert Prozesse für das Role Lifecycle Management.

Kontexte

Kontexte ermöglichen Organisationen die Modellierung und Verwaltung hoch entwickelter organisatorischer Strukturen wie z. B. Matrix-Management-Strukturen oder Organisationen, in denen Mitarbeiter mehrere organisatorische Zugehörigkeiten haben wie Linienaufgabe und Zugehörigkeit zu einem Projekt. Wie Rollen machen auch Kontexte das Managen von User-Gruppen einfacher, da dann alle Mitglieder als eine Einheit verwaltet werden können. Sie sind jedoch verschieden, weil das Mitglied der Gruppe nicht unbedingt die gängige Mitarbeiterrolle innehat, sondern eine auf der Geschäftssituation basierende Rolle. Kontext-Management-Prozesse innerhalb von IdentityPROCESS+ ermöglichen Personen eine Mitwirkung in mehreren Projektteams oder die Wahrnehmung von Sonderaufgaben, die über ihre normale Position hinausgehen. Mit dem Kontext können verschiedene Berechtigungen einhergehen. Ein Kontext kann beispielsweise eine Abteilung, ein Projekt, eine Kostenstelle oder ein Gebäude sein. Diese Prozesse unterstützen auch die Governance organisatorischer Kontexte während deren gesamter Lebensdauer.

Regeln

Regeln oder Policies decken ein breites Spektrum an Governance-Anforderungen innerhalb eines IGA-Paketes ab, u.a. Funktionstrennung (SoD), Vergabe von Zugriffsrechten sowie Datenklassifizierung. Policies lassen sich einzelnen Usern, Kontexten oder Rollen zuweisen und sind Voraussetzung für eine automatisierte, regelkonforme Access Policy, wie sie sowohl von internen Policies als auch externen Bestimmungen wie z. B. SoX, HIPAA, CoBIT, DSGVO, CCPA, ISO 27001 und von der BaFin gefordert wird. Die Nutzung dieser Regeln und Policies führt zu einer weiteren Automatisierung und Reduktion manueller Administrationstätigkeiten.

Mit Zuweisungs-Regeln soll gesichert werden, dass die den Identitäten zugewiesene Zugriffsberechtigungen im Einklang mit internen Regeln und externen Bestimmungen stehen.

SICHERHEITSVORFALL

Kommt es zu einem Zwischenfall, bei dem eine Organisation den Verdacht hat, dass ein Verstoß vorliegt, möchte das Sicherheitsteam möglicherweise den Zugriff durch eine oder mehrere Identitäten sofort unterbinden, damit sich der Verstoß nicht großflächig ausbreitet.

Die bei IdentityPROCESS+ verfügbaren Prozesse im Bereich Sicherheitsvorfälle definieren eine Notfallsperrung so, dass der Administrator den Zugriff eines Users auf sämtliche Systeme on-premises und in der Cloud deaktivieren kann.

Risiken von Verstößen begrenzen

Diese systemübergreifende Zugriffssperrung begrenzt das Risiko eines Unternehmens, weiteren Verstößen ausgesetzt zu sein, während eine Untersuchung durchgeführt wird und die Benutzerpasswörter zurückgesetzt werden. Eine Notfallsperrung kann entweder automatisch über den Incident-Response-Prozess oder manuell durch einen Administrator ausgelöst werden.

Stellt ein Administrator einen Verstoß fest, kann er die Notfallsperrung manuell unter Angabe eines Grundes vornehmen, der bei zukünftigen Untersuchungen

zu Sicherheitsverstößen und Audits als Nachweis fungiert. Im Falle eines „Fehlalarmes" kann die Notfallsperrung auditgerecht wieder aufgehoben werden.

Um die richtige Anwendung von Prozessen rund um Sicherheitsvorfälle sicherzustellen, wird empfohlen, die betreffenden Regeln schriftlich niederzulegen. Die korrekte Umsetzung dieser Prozesse wird in einem eigenen Kapitel zu Prozessen rund um Sicherheitsvorfälle erläutert.

GOVERNANCE

Hat eine Person auf Grundlage bestimmter Kriterien – für die interne Regeln und externe Bestimmungen den Ausschlag geben – einmal bestimmte Zugriffsrechte erhalten, ist eine kontinuierliche Rezertifizierung wichtig, um sicherzustellen, dass der ursprüngliche Grund für den Zugriff nach wie vor gegeben ist.

Die Kontrolle und das Führen von Nachweisen, wer warum Zugriff auf welche Ressourcen hat und wer hierzu die Genehmigung erteilt hat ist für alle Organisationen von Bedeutung, die dauerhaft die Anforderungen interner Sicherheits- und Compliance-Policies sowie externe Vorgaben wie DSGVO, CCPA und ISO27001 erfüllen müssen.

Die Governance-Prozesse bei IdentityPROCESS+ geben Organisationen folgende Möglichkeiten an die Hand:

- Manager/System-Eigentümer können ad hoc bzw. zu einem geplanten Zeitpunkt Aussagen darüber treffen, ob Zugriffsrechte für Identitäten, bestimmte Mitarbeitertypen oder Kontexte immer noch gültig sind.
- Erstellung von Berichten über Regelverstöße wie z. B. Konflikte im Bereich Funktionstrennung (SoD).
- Bereitstellen von Berichten über den aktuellen Zugriffsstatus – anwendungsübergreifend für das gesamte Unternehmen und dadurch audittauglich.
- System-Eigentümer um die Klassifikation von Business-Systemen mit Daten bitten, die separat verarbeitet werden müssen – also Daten, für die bestimmte Regelungen gelten oder vertrauliche Daten, für die geeignete Risikoprüfungen durchzuführen sind.
- Erstellung von Berichten über Regelverstöße, wer diese genehmigt hat und welchen geschäftlichen Grund es dafür gab.

Die Governance-Prozesse helfen Organisationen, die Kontrolle darüber zu behalten und Berichte darüber zu erstellen, wer auf welche Daten zugreift und warum dieser Zugriff genehmigt wurde. Dadurch können Organisationen ein hohes Maß an Sicherheit wahren, Regelverstöße effizient erkennen und angehen und Lizenzkosten sparen, wenn Mitarbeiter eine Software nicht mehr nutzen.

ADMINISTRATION

Im Laufe der Zeit setzen Firmen neue Geschäftssysteme ein, um sich an veränderte geschäftliche Anforderungen anzupassen. Wichtig dabei: Diese neuen Anwendungen müssen mit der IGA-Lösung verbunden sein, damit der Zugriff darauf effizient gemanagt und gesteuert werden kann.

Die administrativen Prozesse bei IdentityPROCESS+ ermöglichen Folgendes:

- Effizientes Onboarding neuer Systeme und Anwendungen.
- Anwendung aussagekräftiger Ressourcenbeschreibungen, die es Endbenutzern erleichtern, bei Self-Service-Anfragen die entsprechenden Ressourcen zu finden.
- Angewandtes Anwendungsmanagement.
- Einrichten von Passwort-Reset-Management und Passwortregeln.

Die administrativen Prozesse erleichtern Identity-Administratoren den Überblick über die Anwendungen, die gemanagt werden bzw. deren Onboarding erforderlich ist. Administratoren können sich so auf die Sicherstellung von geeignetem Zugriff auf Anwendungen konzentrieren, anstatt neue Anwendungen zu integrieren und andere Routineaufgaben wahrzunehmen.

AUDITING

Mit dem technologischen Fortschritt in Organisationen hat sich auch Compliance zu einem immer komplexeren Thema entwickelt, das insbesondere Führungskräfte und die Unternehmensleitung beschäftigt. Interne Sicherheitsanforderungen und -Policies können in Kombination mit regulativen Vorgaben zu immer komplexeren Szenarien führen. Auditfähigkeit hat sich zu einem zentralen Aspekt entwickelt, an dem Organisationen den Zugriff auf geistiges Eigentum und Daten kontrollieren und überprüfen. Parallel dazu erstellen sie Berichte mit detaillierten Angaben zu Access Policies und User-Genehmigungen, um ihre Compliance zu wahren und zu dokumentieren.

Organisationen, die ihre IGA-Lösung nutzen, um Business-Regeln und -Policies durchzusetzen, optimieren dadurch ihren Audit-Prozess. Durch den Umstieg von manuellen Audit-Prozessen auf ein höher entwickeltes, automatisiertes

Modell senken sie den Zeit- und Kostenaufwand für ihr Compliance Reporting beträchtlich. Dies ist ein wichtiger Bestandteil der Grundlagen eines Information Security Management Systems (ISMS). Die Möglichkeit zu kontinuierlichem Datenmonitoring und On-demand-Bewertung der Präzision umgesetzter IGA-Prozesse verleiht einer Organisation eine höhere Transparenz. Die Prozesse liefern Auditoren und Executive Stakeholders die Gewissheit, dass Business-Regeln und -Policies tatsächlich umgesetzt werden. Dadurch können Organisationen nachweisen, dass sie die richtige Governance Control anwenden und das Risiko einer Non-Compliance minimiert haben.

Die Auditing-Prozesse bei IdentityPROCESS+ eröffnen Organisationen folgende Möglichkeiten:

- On-demand-Erstellung auditfähiger Berichte mit vollständigem Audit-Log, einem Katalog mit Compliance-Berichten, vertiefte Analysen und Manager-Dashboards.
- Vorlage einer vollständigen Audit Trail und Änderungshistorien von Genehmigungen, Berechtigungsanträgen, Berechtigungen und Rezertifizierungen.
- Erstellen ausführlicher Berichte über Governance-Policies, Unternehmensrollen, Berechtigungen und Zugriffsdaten.
- Erstellen und Ändern von Berichten auf Basis von Daten wie z. B. Zeiträumen, verbundenen Systemen und Identitäten mit grafischen Präsentationen von Daten für Auditoren/Systemadministratoren.
- Jederzeitige Bereitstellung der Einschätzung von Auditoren und Managern über den Compliance Status einer Organisation.

Soll-/Ist-Vergleich

Automatisierte Auditing-Prozesse ermöglichen Reporting und Bewertung von Business-Policies und -Kontrollmechanismen für den Status-Quo der Identitäten und der damit verbundenen Zugriffsrechte im Vergleich zum erwarteten Soll-Zustand. Dadurch können Administratoren und System-Eigentümer über alle Ausnahmen wie z. B. einen ungültigen Identitätsstatus oder die Erstellung von Accounts oder -Permissions in den gemanagten Systemen informiert werden. Darüber hinaus liefern Auditing-Prozesse kontinuierliche Compliance-Kontrollmechanismen, die eine zeitnahe, geordnete Beseitigung von Verstößen gegen eine Policy unterstützen. Wer nach kontinuierlich sichtbarer, nachvollziehbarer Compliance strebt, möchte die Transparenz der operativen Kontrollmechanismen verbessern. Auditoren und Executive Stakeholder können das IGA-System somit zuverlässiger zur Generierung von Business Value einsetzen. Compliance-Regeln werden dadurch wirksamer durchgesetzt und die vollständige KAudit Trail der Zugriffsrechte von Benutzern an sämtlichen Standorten und Cloud-Systemen wird ermöglicht.

SUMMARY

In this first part the IdentityPROCESS+ framework has been summarized to provide a business-level understanding of the different process areas of identity lifecycle management, access management, business alignment, governance, administration, auditing, and identity security breach.

The processes in each of these areas ensure that organizations can implement best practices to:

- Document who has access to what with a justification as to why
- On-board users with correct access rights, and terminate access when it is no longer needed
- Create or change access rights for employees and contractors as they change roles
- Improve efficiency when managing user identities through improved workflows and automation
- Perform ad hoc and periodic auditing, reviews, and analysis to ensure that users have the right access to the appropriate systems to do their jobs

Kapitel 2

IGA Best Practices im Detail

In Kapitel 1 wurde erwähnt, dass im Zuge des digitalen Wandels immer mehr Unternehmen hybride IT-Umgebungen einsetzen, um effektiv zu sein und ihre Effizienz auf einem von immer mehr Wettbewerb geprägten Markt zu verbessern. Beim Managen von Identitäten und des Zugriffs auf verschiedene Anwendungen, Clouds, Netzwerke und Server treten jedoch unerwartete Herausforderungen auf.

Typische Herausforderungen sind:

- Ein Mangel an adäquaten Sicherheitsvorkehrungen, obwohl sich Organisationen intensiv darum bemühen, dass die Anwendungen on-premises und in der Cloud strikte Identity- und Zugriffs-Sicherheitsanforderungen erfüllen.
- Nicht-Erfüllung von Vorgaben in Bereichen, in denen es Organisationen schwerfällt, Access-Governance-Policies und obligatorische automatisierte Verfahren umzusetzen, die sicherstellen, dass sie alle internen und externen Vorgaben erfüllen.
- Effizient bleiben – Organisationen sind bemüht, die schnelle Implementierung und sicheres Onboarding neuer, digitalisierter Geschäftsprozesse, Systeme und Anwendungen zu gewährleisten.

Identity Governance & Administration (IGA) bewältigt diese Herausforderungen – doch wie bei allen auf Unternehmensebene eingeführten Anwendungen sind auch für ein solches Projekt zur erfolgreichen Implementierung zahlreiche Skills erforderlich. Die Implementierung einer IGA-Lösung umfasst und betrifft zahlreiche Abteilungen im gesamten Unternehmen, erfordert eine technische Integration in zahlreiche andere Software-Produkte, betrifft ein breites Spektrum an Stakeholdern inner- und außerhalb des Unternehmens.

Organisationen müssen sicherstellen, dass ihnen alle Skills zur Verfügung stehen, die sie für den Erfolg brauchen. Es gibt nämlich auch mögliche Stolpersteine, die bedacht werden müssen. Um diese zu umgehen, sollte man u.a. die richtigen Stakeholder einbinden, Best Practices anwenden, nicht überambitioniert vorgehen und die Bedeutung der Datenqualität richtig einschätzen.

Hier setzt das Best-Practice-Framework von IdentityPROCESS+ an – es hilft Organisationen, bei der Umsetzung erfolgreicher IGA-Projekte häufige Stolpersteine zu umgehen. Das Framework liefert Best Practices für jeden Prozess – vom Identity-Management bis hin zu den Zugriffsrechten während der gesamten Zeit, die ein Mitarbeiter im Unternehmen verbringt. Das schafft Zuverlässigkeit bei Governance, Benutzer-Zugriffsverwaltung in hybriden Umgebungen, dem Alignment von Identity-Management mit dem Unternehmen und beim Schutz wichtiger digitaler Assets vor und nach Entdeckung potenzieller Verstöße.

In diesem Kapitel werden die sieben Bereiche von IdentityPROCESS+ Access Management, Business Alignment, Sicherheitsvorfällen, Governance, Administration sowie Auditing, die in Kapitel 1 eingeführt worden waren, detaillierter beschrieben. Wenn jeder der Prozesse im IGA-System implementiert wird, liefern diese eine Funktionalität zur Erfüllung spezifischer Anforderungen unter Gewährleistung entsprechender Sicherheit, Compliance mit internen Policies und externen Bestimmungen sowie einem effizienten Vorgehen beim Onboarding und Verwalten von Identitäten und deren Zugriffen.

Nach Lektüre dieses Kapitels verfügen IT-Sicherheitsexperten über ein umfassendes Verständnis sowohl der verschiedenen Prozessbereiche als auch der Einzelprozesse, die zur erfolgreichen Umsetzung eines kompletten IGA-Systems vorhanden sein müssen.

HINWEISE ZUM AUFBAU DIESES KAPITELS

Das Best-Practice-Framework von IdentityPROCESS+ ist in sieben IGA-Themenbereiche aufgeteilt, die als Prozessbereiche bezeichnet werden.

Die Beschreibung jedes Prozessbereichs in diesem Kapitel lässt sich in drei Teilbereiche unterteilen:

1. Eine Einführung, die beschreibt, wie der Prozessbereich bestimmte geschäftliche Anforderungen umsetzt.
2. Beschreibungen der logischen Prozessgruppen und der Prozesse, die diese enthalten.
3. Beschreibungen zur Art und Weise, wie Stakeholder eingebunden werden sollten und der zentralen Best Practices, die bei der Implementierung der Prozesse umzusetzen sind.

Jeder einzelne Prozessbereich von IdentityPROCESS+ ist miteinander verbunden. Jeder dieser Abschnitte wurde als Einzeltext verfasst. Sie müssen also nicht in einer bestimmten Reihenfolge gelesen werden.

Am Schluss dieses Kapitels findet sich noch ein Abschnitt mit Tipps, wie eine Organisation erste Schritte zur Implementierung von IGA unter Anwendung des IdentityPROCESS+ Framework unternehmen kann. Hier werden die Prozesse beschrieben, auf die man sich konzentrieren sollte, um eine aussagekräftige Übersicht über die Identitäten in einer Organisation und deren Zugriffsrechte zu erhalten.

TERMINOLOGIE

In diesem Abschnitt werden zahlreiche IGA-spezifische Begriffe eingeführt. Würden wir jeden bei der ersten Nennung mit einer Definition versehen, hätte dies negative Konsequenzen für die Lesbarkeit des Textes. Stattdessen findet sich am Ende des Kapitels ein Glossar mit den Fachbegriffen.

Prozessbereich

Identity Lifecycle Management

Ein wesentlicher Bestandteil der Sicherung der Infrastruktur einer Organisation besteht darin, zu gewährleisten, dass Benutzer-Identitäten korrekt erstellt, geändert und deaktiviert werden, wenn ein Mitarbeiter in die Firma eintritt, die Abteilung wechselt, befördert wird oder das Unternehmen verlässt. Identity Lifecycle Management-Prozesse ermöglichen die Vergabe von Zugriffsrechten nach vorgegebenen Rollen, Regeln und Policies, um sicherzustellen, dass Mitarbeiter jederzeit über die passenden Zugriffs-Levels verfügen. Die Aufgabe, den richtigen Benutzerzugriff sicherzustellen, klingt zunächst einfach, doch wie die nachstehende Abbildung zeigt, gestaltet sie sich schnell komplex: Die Abbildung zeigt den Lebenszyklus der Identität einer Person, die dem Unternehmen als Externer beigetreten ist, dann als Mitarbeiter übernommen wurde, in eine andere Abteilung wechselte, befördert wurde, Elternzeit nahm und schließlich das Unternehmen verließ. In jeder Phase der Tätigkeit der Person verlangt die Position Zugriff auf andere Ressourcen im Unternehmen.

Warum Identity Lifecycle Management wichtig ist:

1. Es stellt sicher, dass Mitarbeiter stets den passenden Zugriff haben, den sie benötigen, um ihre Aufgaben korrekt wahrzunehmen.
2. Zur Durchsetzung von regelkonformem Zugriff, bei dem gewährleistet ist, dass Mitarbeiter nicht auf Systeme oder Daten zugreifen, die nicht für sie bestimmt sind.
3. Zur jederzeitigen Durchsetzung des „Least-Privilege"-Prinzips.
4. Zur Begrenzung der Auswirkung im Falle einer Gefährdung von Benutzerkonten.
5. Zur Protokollierung und Nachverfolgung der Frage, wer welchen Zugriff warum gewährt hat.

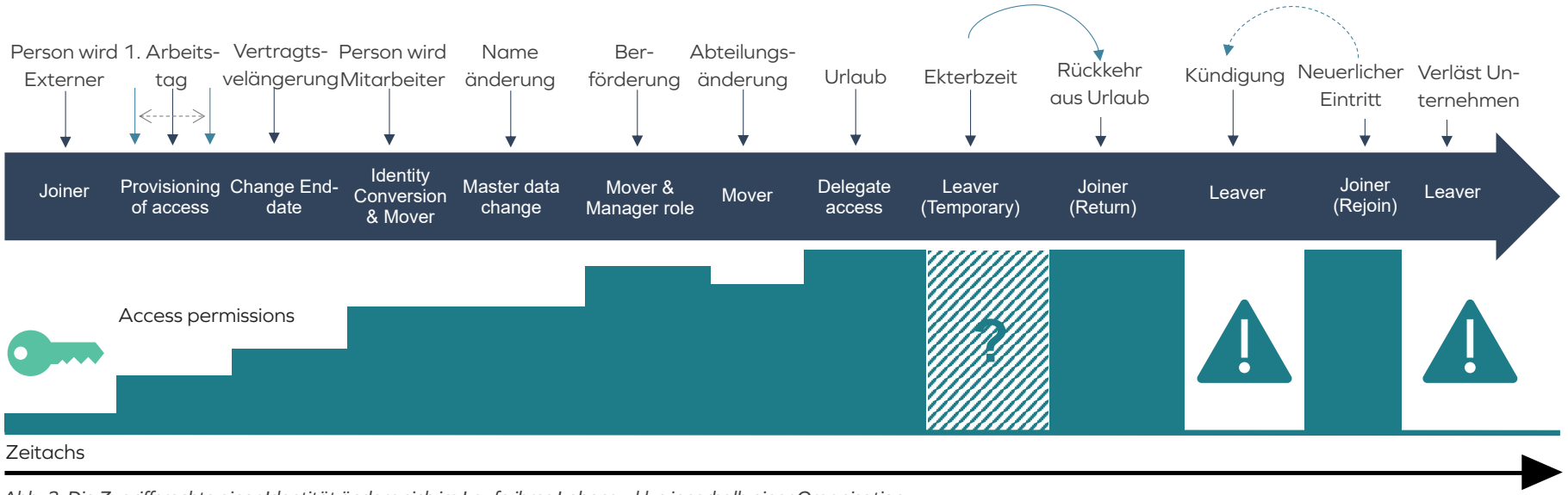


Abb. 2: Die Zugriffsrechte einer Identität ändern sich im Laufe ihres Lebenszyklus innerhalb einer Organisation

Management

des Identity Lifecycles

Prozesse des Identity Lifecycle Management umfassen alle berechtigungs-relevanten Prozesse während der gesamten Tätigkeitsdauer einer Person im Unternehmen. Automatisierte Prozesse stellen sicher, dass Mitarbeiter beim Eintritt in ein Unternehmen Zugriff zu sämtlichen Systemen, Anwendungen und Dateiensystemen erhalten, die sie zur Ausübung ihrer Tätigkeit brauchen. So sind sie vom ersten Tag an produktiv. Wenn Mitarbeiter ihre Position wechseln oder befördert werden, kann ihr Zugriff auf vorhandene Systeme im Verhältnis zur in der neuen Rolle dazugekommenen Verantwortung steigen. Ebenso kann der Wechsel in eine andere Abteilung einen veränderten Zugriff auf bestehende oder neue Systeme mit sich bringen. Schließlich kann es auch erforderlich sein – und stellt sicher auch eine Best Practice dar –, jeglichen Zugriff auf Systeme zu beenden, den ein Mitarbeiter in einer früheren Position hatte, den er aber in der neuen Rolle nicht mehr braucht. Somit häufen sich im Laufe der Zeit keine Zugriffsrechte an. Werden Zugriffsrechte nicht systematisch entfernt, kann es zur Verletzung von Sicherheitsbestimmungen und Compliance-Policies z. B. Im Bereich SoD (Funktionstrennung) kommen. Dieses Off-Boarding von Zugriffsrechten wird auch im Prozessbereich Identity Lifecycle Management behandelt.

Ausbau der Schutzmechanismen

Das Handling von On-Boarding-, Änderungs- und Off-Boarding-Prozessen stellt nicht nur sicher, dass ein Mitarbeiter seine Aufgaben im Job erfüllen kann, sondern hat den zusätzlichen Vorteil, dass Eindringlinge bei Gefährdung eines Benutzerkontos nur begrenzten Zugriff auf Systeme erhalten. Die durch diese Prozesse geschaffene Sicherheitsgrenze schafft über die herkömmlichen Sicherheitsmaßnahmen wie z. B. Firewalls und Intrusion- Prevention-Systemen hinaus zusätzliche Sicherheit. Das Identity Lifecycle Management konzentriert sich nicht rein auf Mitarbeiter – das tatsächliche Umfeld ist nämlich oft komplexer, da Unternehmen in der Regel auch Externe wie z. B. Lieferanten, Saisonarbeiter oder Geschäftspartner mitverwalten müssen, die ebenfalls Zugriff auf Unternehmensressourcen benötigen, um dort effizient tätig sein zu können.

Würde man diesen ganzen Lebenszyklus manuell verwalten, würde dies beträchtliche IT-Ressourcen zur Provisionierung bzw. Deprovisionierung individueller Accounts binden. Eine manuelle Verwaltung ist fehleranfälliger und würde das Unternehmen unnötigen Sicherheits- und Compliance-Risiken aussetzen. Stattdessen automatisiert die Omada Identity Suite (OIS) mit IdentityPROCESS+ die Prozesse zum Management aller nachstehend aufgeführten Aspekte des Identity Lifecycle Management. Die im Prozessbereich Identity Lifecycle Management vorkommenden Prozesse sind als Joiner-Mover-Leaver-Prozesse bekannt. Grund: Dieser Prozessbereich macht es Organisationen möglich, die Identitäten von Mitarbeitern oder Externen zu erstellen, zu ändern und wieder zu terminieren. Allen Prozessen gemein ist, dass das Auslösen eines beliebigen Prozesses zur Aktualisierung der Identitäten gemäß Security Levels, Business Policies, Position, Organisations-Hierarchie und Kontext führt.

Der gesamte Prozessbereich Identity Lifecycle Management umfasst die folgenden Prozesse:

Onboarding Identity (Prozess)

- Hinzufügen eines Mitarbeiters (untergeordneter Prozess)
- Hinzufügen eines externen Mitarbeiters
- Hinzufügen einer technischen Identität

Änderungen der Identity

Organisationsinterner Transferprozess

- Änderungsprozess Masterdaten

Off-board-Identity

- Terminierung

(Daten und Prozesse sind von der Identität nicht mehr ein- und du chführbar, die Identität ist nicht mehr sichtbar im System. Die Historisierung gemäß gesetzlichen Vorgaben erfolgt.)

Prozess

Onboard Identity

Automatisiert die Erstellung von Identitäten für Mitarbeiter oder Externe, wenn diese ihre Zusammenarbeit mit dem Unternehmen beginnen und ermöglicht die Erstellung technischer Identitäten zum Managen von Geschäftssystemen.

NEUEN MITARBEITER HINZUFÜGEN

Dieser Prozess stellt sicher, dass der neue Mitarbeiter vom ersten Tag an produktiv ist und Zugriff zu allen Systemen hat, um seine Aufgaben zu erledigen.

Prozessbeschreibung

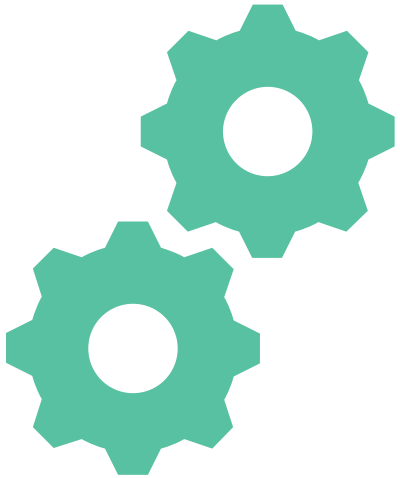
Der Onboard-Identity-Prozess generiert automatisch eine neue Identität, wenn im Master-HR-System ein neuer Personalstammdatensatz angelegt wird. Die Identität wird vordefinierten Zugriffsrechten zugewiesen, die nicht nur Zugriff auf die Ressourcen gewähren, die zunächst allen Mitarbeiter zur Verfügung stehen – wie z. B. Active Directory, E-Mail, relevante gemeinsam genutzte Festplatten sowie das Bonussystem des Unternehmens –, sondern auch auf Spezialanwendungen wie die Einkaufsanwendung oder Entwickler-Tools, die je nach Rolle oder Kontext eingesetzt werden.

Best-Practice-IGA-System-Funktionalität

Die neue Identität besteht aus einem eindeutigen Benutzernamen und wird automatisch in das IGA-System importiert und dort verarbeitet. Für die neue Identität zuständige Person – z. B. den Manager oder Administrator – wird eine Genehmigungsaufgabe erstellt, damit der Onboarding-Prozess bestätigt und genehmigt werden kann. Die Identität wird im System bis zum „Gültig ab"-Datum als inaktiv gesetzt. Die Identität wird beim Erreichen des „Gültig ab"-Datums als aktiv gesetzt.

Technischer Prozessablauf

1. Bei Eintritt eines neuen Mitarbeiters erstellt die Personalabteilung einen Personalstammdatensatz in einem Quellsystem, z. B. in einem HR-Management-System.
2. Dieser Personalstammdatensatz wird automatisch in das IGA-System importiert.
3. Die Schritte des Workflows erfolgen automatisch.
4. Das IGA-System liest den Personalstammdatensatz und verarbeitet sie nach vordefinierten Zuweisungs-Regeln.



EXTERNE HINZUFÜGEN

Externe und andere vorübergehend Beschäftigte sind ein wichtiger Bestandteil der Tätigkeit eines Unternehmens. Das Managen von deren Identitäten ist ebenso notwendig wie bei Vollzeitangestellten – auch hier gilt es, sie vom ersten Tag an unter Zugriff auf die richtigen Systeme und Ressourcen produktiv arbeiten zu lassen.

Prozessbeschreibung

Dieser Prozess ähnelt dem zuvor beschriebenen Onboard-Employee-Prozess. Der für den Externen zuständige Manager erstellt eine neue Identität und gibt an, auf welche Systeme und Ressourcen der Lieferant Zugriff haben sollte. Ein wichtiger Teil dieses Prozesses, der vom Managen von unbefristet Angestellten abweicht: bei Externen muss das Anfangs- und Enddatum der Tätigkeit angegeben werden, um sicherzustellen, dass die Identität nur während der Vertragslaufzeit Zugriff auf relevante Daten hat. Nach erfolgter Genehmigung hat der Externe während seiner Tätigkeit für das Unternehmen Zugriff zu den relevanten Daten.

Best-Practice-IGA-System-Funktionalität

Der Onboard-Contractor-Prozess wird bei Untervertragnahme eines neuen Externen vom Abteilungsleiter manuell eingeleitet. Die Identität kann aber auch im HR-System erstellt werden, wenn hier die Externen verwaltet werden. Ansonsten kann die Identität auch direkt im IGA-System erstellt werden. Das IGA-System erkennt dabei automatisch, dass bereits eine Identität mit ähnlichen Masterdaten vorliegt, weil ein Externer schon zuvor für das Unternehmen tätig war. Liegt bereits eine ähnliche Identität vor, kann der Manager entweder eine neue Identität erstellen oder die vorhandene aktualisieren. Werden ein Start- und ein Enddatum angegeben, aktiviert bzw. terminiert das IGA-System automatisch den Zugriff auf die jeweiligen Daten. In der aktiven Periode der Identität kann der Externe direkt im IGA-System auch zusätzliche Zugriffsrechte anfordern; hierzu wäre dann die Genehmigung durch den Manager erforderlich.

Technischer Prozessablauf

1. Ein Benutzer mit entsprechenden Rechten löst manuell den Onboard-Contractor-Prozess aus, indem er ein Online-Formular mit den persönlichen Daten des Externen ausfüllt.
2. Der Benutzer versendet das Formular, das IGA-System prüft auf evtl. Konflikte und Überschneidungen.
3. Besteht bereits eine Identität mit ähnlichen Masterdaten wie z. B. Name oder E-Mail-Adresse hat der Benutzer die Möglichkeit, eine neue Identität zu erstellen, die bestehende zu aktualisieren oder den Prozess abzubrechen.
4. Die Anfrage wird zur Genehmigung übersandt.

! QUICK WIN...

Richtiger Zugriff gleich vom ersten Tag an: Werden geeignete Zuweisungsregeln definiert, erhält die neue Identität automatisch grundlegende Zugriffsrechte – mit minimalem Aufwand von IT- und Personalabteilung und Personalverantwortlichen.

ONBOARD TECHNICAL IDENTITY

Damit man Mitgliedern des IT-Teams keine Administratorenrechte für Systeme ihrer persönlichen Identitäten zuordnen muss, werden technische Identitäten verwendet. Da technische Identitäten privilegierte Zugriffsrechte haben und von mehreren IT-Usern verwendet werden, müssen sie einem Eigentümer zugewiesen werden, der für die Governance des Accounts zuständig ist.

Prozessbeschreibung

Um sicherzustellen, dass diese oft mächtigen technischen Identitäten korrekt gemanagt werden, ermöglicht der Onboard-Technical-Identity-Prozess es System-Eigentümern, einen Account einzurichten und die Zuständigkeit dafür einem tatsächlichen User zuzuweisen, der als Primäridentität bezeichnet wird. Diese Zuweisung sichert die Aufrechterhaltung einer engmaschigen Governance, da die Primäridentität auch dann für die Ressource zuständig ist, wenn zahlreiche andere User auf das System zugreifen und denselben Account verwenden.

Best-Practice-IGA-System-Funktionalität

Der System-Eigentümer füllt das technische Abfrageformular im IGA-System aus, das hieraus dann die technischen Standard-Eigenschaften der Identität erstellt. Die technische Identität wird dann einem Eigentümer (der Primäridentität) zugewiesen (Mapping), der für den Account zuständig ist. Ist dieses Mapping vollzogen, ist die technische Identität bereit und die User können Zugriffsanträge stellen, um die technische Identität zur Durchführung von administrativen Aufgaben im System einzusetzen.

Technischer Prozessablauf

1. Der System-Eigentümer beantragt neue technische Identitäten für seine Systeme durch Ausfüllen des Antragsformulars für technische Identitäten
2. Die technische Identität wird erstellt, die Standardeigenschaften werden zugewiesen
3. Die technische Identität wird auf den Eigentümer (der Primäridentität) gemappt
4. Die technische Identität ist bereit für Zugriffsanträge von Usern

! QUICK WIN...

Engmaschige Governance sichern: Zuweisung der Eigentümerschaft für technische Identitäten mit privilegierten Zugriffsrechten an tatsächliche User.

Prozess

Änderungen der Identity

Verwaltet die Zugriffsrechte von Mitarbeitern und Externen, wenn diese andere Funktionen übernehmen oder die Abteilung im Unternehmen wechseln sowie die Änderung persönlicher Mitarbeiterdaten.

ORGANISATIONSINTERNER TRANSFER

Wechselt ein Mitarbeiter oder Lieferant innerhalb einer Organisation in eine andere Abteilung oder erfolgt eine Beförderung, müssen die Zugriffsrechte des Betreffenden überprüft und aktualisiert werden, um sicherzustellen, dass der Mitarbeiter nur Zugriff zu den Systemen hat, auf die er zugreifen soll. Dies verhindert, dass während des Wechsels bestimmte Kombinationen aus von den Unternehmens-Policies verbotenen Zugriffsrechten wie z. B. Funktionstrennung (SoD) gewährt werden.

Prozessbeschreibung

Wechselt ein Mitarbeiter oder Lieferant von einer Unternehmensabteilung in eine andere oder erfolgt eine abteilungsinterne Beförderung, widerruft der organisationsinterne Transferprozess die Zugriffsrechte für die alte Rolle und fügt Rechte für die neue Rolle hinzu. Nach Durchführung eines Wechsels erfolgt die Genehmigung durch den Vorgesetzten der/des Betreffenden, der bei Bedarf alle direkten Berechtigungs-Zuweisungen löschen kann.

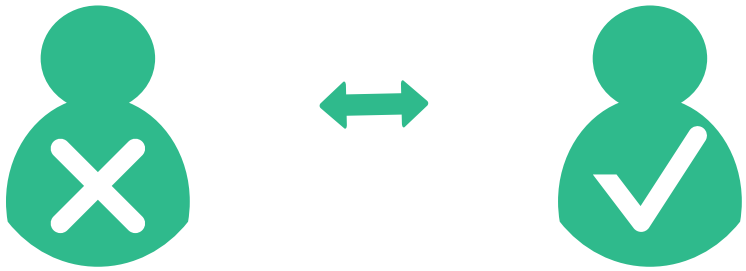
Best-Practice-IGA-System-Funktionalität

Der Prozess wird eingeleitet, wenn ein Mitarbeitertransfer oder eine Beförderung in das HR-System (das Quellsystem) eingegeben wird. Dieses Ereignis führt dazu, dass das IGA-System klärt, welche neue Rollen dem Account eines Mitarbeiters hinzugefügt bzw. welche deaktiviert werden sollten. Ist dieser Schritt abgeschlossen, ist der Account bereit für die Genehmigung oder weitere Änderungen durch den Abteilungsleiter. Der Manager hat die Option, je nach Position Zugriffe hinzuzufügen oder zu entziehen. Zugriffsrechte werden in den Systemen automatisch provisioniert bzw. deprovisioniert.

Entzogene Zugriffsrechte bleiben standardmäßig über einen vordefinierten Zeitraum bestehen; so erhält der User die Möglichkeit, auf Arbeitsaufträge zuzugreifen und diese zu übergeben.

Technischer Prozessablauf

1. Die Änderung einer Position wird in das HR-System / Quellsystem eingegeben.
2. Regeln und Policies für die neue Position erfüllende Zugriffsrechte werden automatisch auf das Konto des Mitarbeiters angewandt.
3. Der Manager erhält eine Benachrichtigung zur Änderung der Zugriffsrechte für das Konto des Mitarbeiters.
4. Nach Genehmigung durch den Manager werden neue Zugriffsrechte auf den Account des Mitarbeiters angewandt.
5. Nachdem eine zuvor festgelegte Frist vergangen ist, verliert der Mitarbeiter sämtliche Zugriffsrechte, da der Manager keine Rezertifizierung vorgenommen hat.



ÄNDERUNG VON STAMMDATEN

Die Stammdaten sind in einem zentralen Datenspeicher gespeichert, der sich aus einem oder mehreren Systemen speist. Das Zusammentragen, Aktualisieren und Managen von Stammdaten kann ein schwieriges Unterfangen sein. Wichtig ist daher eine saubere Stammdatenverwaltung, bei der sichergestellt wird, dass Datenänderungen von Managern überprüft werden und diese Änderungen auch in sämtlichen Systemen umgesetzt werden.

Prozessbeschreibung

Der Änderungsprozess der Stammdaten verschlankt den Prozess für Änderungsanträge, Updates und Ergänzungen der Stammdaten einer Organisation und stellt sicher, dass Änderungen in Systemen gespeichert werden, die mit dem IGA-System in Verbindung stehen.

Best-Practice-IGA-System-Funktionalität

User können ihre Dateneinträge ändern. Diese Änderungen sind vom Manager der Identität zu genehmigen. Erkennt das IGA-System eine Änderung in den Stammdaten, wird der Änderungsprozess initiiert, bei dem die veränderten Daten eingesammelt und in der IGA-Lösung nach vordefinierten Daten-Mapping-Regeln aktualisiert werden. Alle Änderungen der Stammdaten einer Identität werden dann auf Grundlage vordefinierter Provisionierungsregeln automatisch auch in den verbundenen Systemen übernommen.

Technischer Prozessablauf

1. Ein/e Mitarbeiter/in ändert seine/ihre persönlichen Daten.
2. Die Änderung wird dem für Datenänderungen des/der betreffenden Mitarbeiters/Mitarbeiterin verantwortlichen Manager per Event-Mitteilung kommuniziert.
3. Der Manager lehnt die Änderungsanfrage ab bzw. genehmigt sie; bei Genehmigung wird die Änderung auch in anderen Systemen/Untersystemen übernommen.

! QUICK WIN...

Stammdaten-Governance: Sicherstellen, dass Datenänderungen geprüft und in allen Systemen angewandt werden.

Prozess

Off-Board-Identity

Verwaltet das Off-Boarding von Mitarbeitern, wenn diese kündigen oder entlassen werden, wodurch diese nach Verlassen der Firma keinen Zugriff mehr auf Anwendungen haben.

TERMINIERUNG

Organisationen müssen sicherstellen, dass Mitarbeiter und Externe keinen Zugriff mehr auf Systeme haben, nachdem sie die Zusammenarbeit mit dem Unternehmen – sei es vorübergehend oder dauerhaft – beendet haben.

Prozessbeschreibung

Der Terminierungsprozess deckt sowohl das unmittelbare Off-Boarding von Mitarbeitern oder Externen als auch das geplante permanente Off-Boarding ab, das Anwendung findet, wenn ein Benutzer gekündigt hat und während der Kündigungsfrist noch Zugriff auf die Systeme benötigt. Der Prozess automatisiert die Terminierung von Zugriffsrechten bzw. deaktiviert Anwendungen in den Systemen und stellt dabei sicher, dass diese korrekt deprovisioniert werden und Benutzer nach ihrem Ausscheiden aus dem Unternehmen nicht mehr auf Daten zugreifen können.

Best-Practice-IGA-System-Funktionalität

Der Prozess wird ausgelöst, wenn:

- Das „Gültig bis"-Datum im Identitätsdatensatz des HR Systems oder der IGA-Lösung erreicht ist. Dies passiert beispielsweise bei Externen mit vordefinierten Enddaten.
- Diese Identitätsakte vom Quellsystem nicht mehr zur Verfügung gestellt wird. Dies passiert, wenn der Datensatz deaktiviert wird, nachdem der betreffende Mitarbeiter das Unternehmen verlassen hat.

Wird der Prozess absichtlich oder unabsichtlich ausgelöst, wird in beiden Szenarien die Identität deaktiviert, alle entsprechenden Konten deaktiviert und der Zugriff verweigert.

Ist ein Konto einmal deaktiviert, beginnt der Prozess der Eigentumsübertragung, die im Verantwortungsbereich des deaktivierten Kontos liegenden Ressourcen auf andere User zu übertragen.

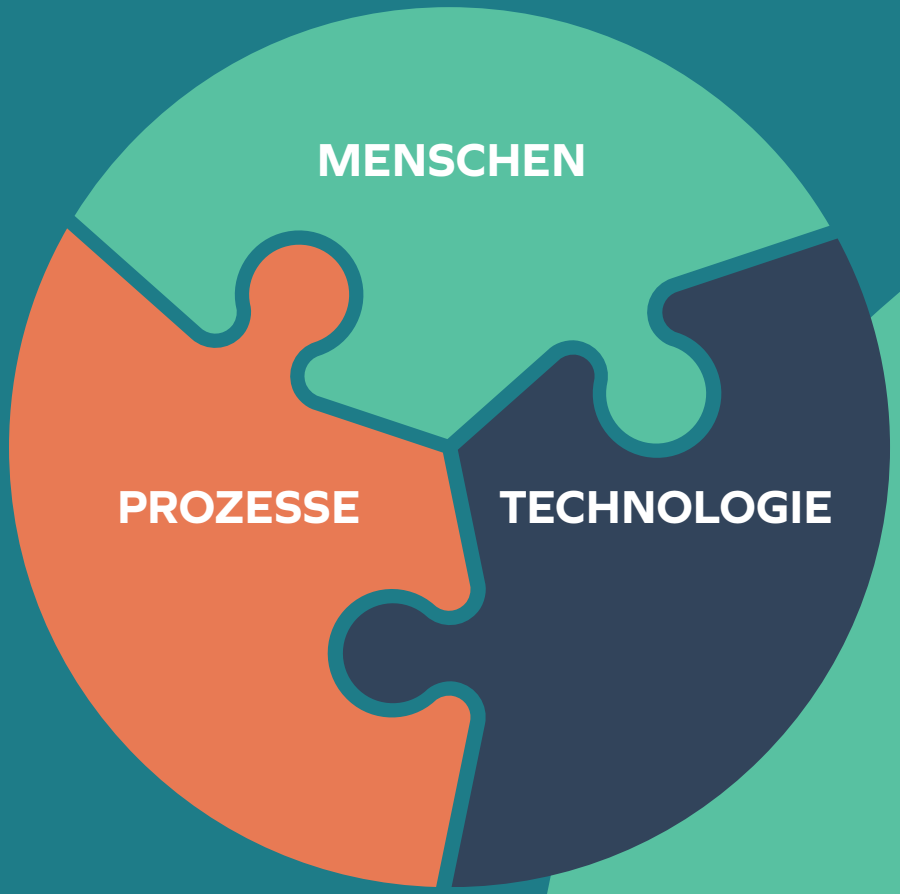
Technischer Prozessablauf

1. Das „Gültig bis"-Datum im Identitätsdatensatz des HR Systems oder der IGA-Lösung ist erreicht, oder ein fehlender Datensatz löst den Prozess in der IGA-Lösung aus.
2. Der Identitätsstatus wird auf „terminiert" gesetzt.
3. Die Identität wird deaktiviert, alle ihre Konten deaktiviert und der Zugriff verweigert.
4. Der Transfer-Ownership-Prozess wird im IGA-System ausgelöst, um sicherzustellen, dass alle Ressourcen, die bis dahin im Besitz der deaktivierten Identität waren, neu zugewiesen werden.

Implementieren von Best Practices

Identity Lifecycle Management

Zur erfolgreichen Implementierung von Identity Lifecycle Management müssen die jeweiligen Stakeholder mitwirken und nach gründlicher Voranalyse Daten, Regeln und Policies definiert werden. So lassen sich Prozesse an die organisatorische Struktur anpassen.



PROZESS-STAKEHOLDER

Da Definition und Implementierung des Identity Lifecycle-Management-Prozesses zahlreiche Abteilungen umfassen, ist es wichtig, sicherzustellen, dass die relevanten Stakeholder in einer frühen Projektphase eingebunden und über ihre Beteiligungen und Pflichten informiert werden. Das Kommunizieren dieser Erwartungen stellt sicher, dass alle am Prozess Beteiligten angesprochen und Identity Lifecycle Management-Prozesse reibungslos implementiert werden. Die folgende Tabelle zeigt eine Liste von Stakeholdern im Prozessbereich Identity Lifecycle Management und führt die Beteiligung, Verantwortlichkeiten und Aufgaben auf, die von ihnen vor und nach der Implementierung erwartet werden.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
Personalabteilung (HR)	Die Personalabteilung ist sowohl bei Projektbeginn als auch im Laufe des gesamten IGA-Projektes involviert. Die Arbeit der Personalabteilung umfasst alle Aspekte des Identity Lifecycle Management, da HR-Daten eine Schlüsselrolle bei allen Prozessen zukommt.	Die Personalabteilung ist bei Beginn beteiligt, um die Integrität der Daten im HR-System (Quellsystem) zu gewährleisten, da diese die Grundlage für die Zuweisung von Rollen und somit auch Zugriffsrechten für Personen sind. HR liefert die Stammdaten an OIS. Nach der Installation sind sie auch an der Durchführung von Änderungen an Mitarbeiterdaten beteiligt, die im IGA-System zur Provisionierung bzw. Deprovisionierung von Zugängen verwendet werden.	1) Sicherstellen, dass Mitarbeiterdaten korrekt und stimmig sind. 2) Das IGA-Team benötigt entsprechenden Zugriff, damit es Daten aus dem Quellsystem in das IGA-System importieren kann.	1) Saubere Erfassung der Daten neuer Mitarbeiter im HR System, damit das IGA-System ebenso präzise Zugriffsrechte gewähren kann. 2) Vornehmen von Änderungen an Mitarbeiterdaten, um deren aktuellen Status widerzuspiegeln (z. B. derzeitige Position, Manager). 3) Sicherstellen von konsistentem Daten-Input zur Wahrung der Dateninteg rität – so laufen IGA-Prozesse reibungslos.
IGA-Team	Das IGA-Team arbeitet bei IGA-Projekten schon früh mit der Personalabteilung zusammen, da sie die Datenintegrität im Quellsystem (HR-Daten) sicherstellen müssen, bevor diese in das IGA-System übertragen werden. Das IGA-Team ist nicht direkt in Identity Lifecycle Management-Prozesse von HR involviert.	Das IGA-Team muss die Integrität der in das IGA-System importierten Mitarbeiterdaten überprüfen, da diese die Basis zahlreicher Prozesse sind. Ohne Datenintegrität wären die Prozesse im Bereich Identity Lifecycle Management unzuverlässig, weil sie auf ungenauen Daten basieren würden.	1) In Zusammenarbeit mit der Personalabteilung saubere Datensätze sicherstellen. 2) Integrieren des HR-Systems und anderer potenzieller Quellsysteme in das IGA-System.	Überprüfung der Integrität von Datenimporten.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
Mitwirkung von Vorgesetzten	Die Mitwirkung von Vorgesetzten beginnt, sobald die HR-Daten in das IGA-System geladen wurden. Mit Blick auf Identity Lifecycle Management sind sie am Genehmigungsprozess beim Onboarding von Mitarbeitern, Externen, bei organisations-internen Transferprozessen, Stammdatenänderungen und der Terminierung von Benutzer- Identitäten beteiligt.	Da Vorgesetzte am besten wissen, wie ihre Abteilung funktioniert, sind sie in der idealen Position, Rollen zu definieren und Zugriffsanträge von Usern zu genehmigen bzw. abzulehnen und die Änderung von Stammdaten zu genehmigen.	Work with the IGA team and Business System Owners to define roles based on their knowledge of the employees in their department.	Genehmigung der Einführung von Mitarbeitern und Externen, organisationsinternen Transferprozessen, Änderung von Stammdaten sowie der Terminierung von User Identitäten.
Endbenutzer (Mitarbeiter und Externe)	Nach Implementierung des IGA-Systems kann die Mitwirkung von Endbenutzern in einem beliebigen Prozess des Identity Lifecycle Management beginnen.Manchmal (beim Einführen von Mitarbeitern, Externen, organisationsinternen Transferprozessen und Kündigungen) sind sie aber auch indirekt beteiligt, da ihr Manager in ihrem Namen in einen Prozess involviert ist; in anderen Fällen jedoch (bei Änderung von Stammdaten) interagieren sie direkt mit dem Prozess.	An Prozessen im Bereich Identity Lifecycle Management sind auch End-User beteiligt, wenn diese in das Unternehmen eintreten, in andere Positionen wechseln, das Unternehmen verlassen oder wenn sie Änderungen an den persönlichen Daten vornehmen müssen.	Keine	Bei Bedarf Änderung persönlicher Stammdaten.
Eigentümer von Anwendungen	Nach Übertragung der HR-Daten in das IGA-System beginnen die Eigentümer von Anwendungen zusammen mit dem IGA-Team mit dem Onboarding von Anwendungen im IGA-System. Beim Lifecycle Management von Entities erstellen Eigentümer von Anwendungen mit dem Prozess "Hinzufügen einer technishe Identitäten für die Systeme, für die sie zuständig sind.	Eigentümer von Anwendungen wirken an Identity Lifecycle Management-Prozessen mit, weil sie für Sicherheit und Governance ihrer Systeme verantwortlich sind. Daher fällt auch die Erstellung technischer Identitäten in ihren Aufgabenbereich, damit IT-Administratoren auf ihre Systeme zugreifen und diese managen können.	Keine	Erstellen technischer Identitäten, damit IT-Administratoren auf ihre Systeme zugreifen und diese managen können.

Wichtige Best Practices

Empfehlungen

Im Folgenden eine Reihe von Best-Practice-Empfehlungen, die bei der Implementierung von Identity Lifecycle Management-Prozessen in IdentityPROCESS+ bedacht werden sollten.

DATENVERWALTUNG

Definieren von Daten-Qualität

Da Mitarbeiterdaten und Daten von Externen beim Erfolg von IGA-Projekten eine entscheidende Rolle zukommt, gilt es, Regeln zur Steuerung der Daten-Qualität zu definieren. Dies umfasst auch das Identifizieren der Schnittstellen zu den Anwendungen und die Frage, wie sich Datentransfers zwischen diesen und dem IGA-System qualitativ optimieren lassen.

Bestimmen der Quellen von Stammdaten für Personendatensätzen

Jedes IGA-System benötigt Personendatensätze zur Implementierung des IdentityPROCESS+ Frameworks, so z.B. bei Neuzuweisung von Zugriffsrechten an identifizierte Rollen oder das Weiterleiten von Zugriffsanträgen an Vorgesetzte mit Bitte um Genehmigung. Um sicherzustellen, dass diese Prozesse effektiv ablaufen, müssen die richtigen Daten in das IGA-System importiert werden.

Diese Situation kann jedoch durch das Vorhandensein zahlreicher verschiedener Quellen von Personendatensätzen verkompliziert werden. Die erforderlichen Daten könnten:

1. über das Unternehmen verstreut in verschiedenen, unabhängigen Systemen gespeichert, oder
2. im Netzwerk über verschiedene Systeme hinweg doppelt vorhanden sein.

Werden Mitarbeiterdaten in verschiedenen, unabhängigen Systemen gespeichert, müssen zur Übertragung von Daten von jedem Einzelsystem zum IGA-System entsprechende Verbindungen verwendet werden. Liegen Daten jedoch doppelt vor – entweder, weil manche davon im HR-System, andere wiederum im Active Directory gespeichert werden, oder weil zur Verbesserung der Systemleistung ein redundantes System aufgesetzt wurde –, muss die Organisation entscheiden, welches Quellsystem mit Blick auf Attribute die Stammdaten bereitstellt. Diese Entscheidung muss dann im IGA-System implementiert werden, damit jede Information auf eine bestimmte Quelle zurückgeführt werden kann. Für komplexe Umgebungen könnte hierzu eine aufwändige Logik erforderlich sein.

Diese Entscheidung ist eine der ersten Überlegungen, die eine Organisation anstellt, wenn sie eine IGA-Lösung einsetzen möchte, da das IGA-System ohne saubere Daten nicht richtig funktioniert. Darüber hinaus können die Quellen von Mitarbeiterdaten und Daten von Externen sehr komplex sein, weshalb die Organisation die Definition der Stammdatenquellen selbst durchführen muss – diese Aufgabe kann nicht allein von einem IGA-Anbieter oder externen Integrator. durchgeführt werden. IGA-Anbieter arbeiten jedoch mit der Organisation zusammen, um sicherzustellen, dass die Daten die nötigen Anforderungen erfüllen.

Übertragen von Stammdaten vor der Implementierung von Prozessen

Vor der Implementierung von Prozessen sind zunächst alle Stammdaten in das IGA-System zu übertragen. Unterbleibt dies, müssen Prozesse wie die Rezertifizierung nach jedem Data-Load erneut durchgeführt werden – eine zeit- und ressourcenaufwändige Prozedur.

Bestimmen der Häufigkeit von Datenimporten auf Quellsystemen

Datenänderungen im HR-System erfolgen meist, weil Mitarbeiter ins Unternehmen kommen, befördert werden oder das Unternehmen wieder verlassen. Folglich müssen Daten regelmäßig aus der HR-Datenbank (oder einem anderen Quellsystem) in das IGA-System importiert werden. Wie oft ein solcher Import nötig ist, hängt von den geschäftlichen Anforderungen ab. Für die meisten Organisation genügt es in der Regel, diesen Arbeitsschritt einmal täglich durchzuführen. In Organisationen, deren Mitarbeiter noch am selben Tag ein Onboarding vollziehen, kann es jedoch erforderlich sein, die Daten alle zwei bis vier Stunden zu importieren.

IDENTITIES

Sicherstellen, dass Rollen zur Erstellung eindeutiger Identitäten vorhanden sind

Es ist sehr wichtig, dass alle Identitäten im IGA-System eindeutig sind. Besteht keine Policy zur Benennung von Identitäten, muss dies nachgeholt werden. Darüber hinaus sollte die Policy zur Benennung von Identitäten für die gesamte Organisation schriftlich festgehalten werden.

Benutzer-IDs nicht mit Identitätsdaten verknüpfen

Es sollten keine veränderlichen Attribute zur Bildung der ID verwendet werden. So besteht keine Notwendigkeit zur Änderung der Identitäts-ID, wenn z.B. der Name geändert wird.

Verwenden Sie keine alten Benutzer-IDs erneut für im Unternehmen tätige Mitarbeiter und Externe

Für Personen, die das Unternehmen verlassen haben und dann erneut für es tätig sind, sollten andere Benutzer-IDs erstellt werden – unabhängig davon, ob es sich um Mitarbeiter oder Externe handelt. Wird dies so gehandhabt, kann die Organisation sicher sein, dass Protokolle und historische Datensätze separat gespeichert werden und Anträge und Änderungen der Zugriffsrechte korrekt anzeigen. Die neue Benutzer-ID erleichtert bei Unternehmensaudits die Analyse der verschiedenen Anstellungszeiten.

GOVERNANCE AND STANDARDS

Erwägen der Optimierung von Geschäftsprozessen zur Senkung der Komplexität

Die aktuell angewandten Geschäftsprozesse sind einer Bewertung zu unterziehen. Sind diese aufgrund eines bindenden Regulierungsrahmens nicht schriftlich niedergelegt, wird empfohlen, dass die Organisation die Möglichkeit erwägt, veraltete Prozesse zu dynamisieren und Komplexität nach Möglichkeit zu reduzieren.

Hierbei ist zu beachten, dass es innerhalb der Organisation unterschiedliche Prozesse gibt. Weicht ein Prozess für Bankspezialisten von demjenigen ab, den andere Mitarbeiter einsetzen, wird die Standardisierung schwierig. In einem solchen Fall sollte eine Prozessoptimierung erwogen werden.

Prüfung von Prozessen

Die Implementierung einer IGA-Lösung ist ein geeigneter Moment, um Prozesse in der gesamten Organisation auf den Prüfstand zu stellen, um sicherzugehen, dass alle Prozesse darauf ausgerichtet sind, das Unternehmen auch in Zukunft zu unterstützen. Komplexe Situationen lassen sich oft stark vereinfachen und die Gesamteffizienz enorm steigern, wenn veraltete Prozesse abgelöst und andere Prozesse automatisiert werden. Ein Beispiel: Früher mussten Manager im Namen ihrer Mitarbeiter den Zugriff zu Systemen beantragen, da dies die einzige Möglichkeit zur Arbeit im alten IGA-System darstellte. Seit der Einführung von Self-Service-Möglichkeiten können Mitarbeiter jetzt auch ihren eigenen Zugriff zu Anwendungen beantragen – das senkt den Arbeitsaufwand des Managers.

Sicherstellen, dass Standards dokumentiert werden und die aktuellen und zukünftigen rechtlichen Anforderungen erfüllen

Über dokumentierte Standards zu verfügen, ist aus Compliance-Sicht wichtig und hilft, Auditoren gegenüber zu belegen, dass die Organisation die rechtlichen Anforderungen verstanden hat. Bei der Bestandsaufnahme von in der Organisation bereits vorhandenen Standards wird empfohlen, auch eine Analyse der zukünftigen Compliance-Anforderungen vorzunehmen. Das beugt zusätzlichem Arbeitsaufwand vor, wenn neue gesetzliche Regelungen in Kraft treten.

NÜTZLICHE TIPPS

Frühzeitiges Einbinden von Managern in das Projekt

Viele Entscheidungen rund um das Definieren von Identity Lifecycle Management-Parametern brauchen Input von Personen, die die unternehmerischen Anforderungen genau kennen. Diese Anforderungen könnten auch rechtliche und Compliance-Anforderungen umfassen, z. B. um sicherzugehen, dass Daten nur für einen bestimmten Zeitraum aufbewahrt werden, aber auch individuelle Anforderungen für einzelne Länder und Branchen. Daher wird empfohlen, dass Stakeholder aus der gesamten Organisation bereits in der Anlaufphase von IGA-Projekten eingebunden werden, damit die geschäftlichen Anforderungen frühzeitig in die Prozesse integriert werden, anstatt diese erst nach der Implementierung zu integrieren.

Managen von Externen zur Sicherstellung von Compliance

Zur Gewährleistung einer zuverlässigen Governance sollten Organisationen sicherstellen, dass vor Eingliederung eines Externen in das IGA-System eine schriftliche Vereinbarung vorliegt. Ist ein Vertrag vorhanden, hilft dies sicherzustellen, dass der Externe nach den Regeln und Bestimmungen des Unternehmens vorgeht und die Anforderungen von Audits erfüllt. Darüber hinaus wird empfohlen, dass Zugriffsrechte für Externe auf einen absehbaren Zeitraum wie z. B. 3 oder 6 Monate begrenzt werden. Dies ist besonders dann wichtig, wenn die Organisation strengen gesetzlichen Bestimmungen unterworfen ist. Unterbleibt dies, kann es sein, dass der Benutzerzugriff vergessen wird oder ein Externer noch lange nach Beendigung seiner Zusammenarbeit mit dem Unternehmen Zugriff auf Daten hat. Es sind zeitliche Begrenzungen zu definieren, wie lange eine Zugriffsgenehmigung gültig sein sollte – vorzugsweise durch die Personalabteilung.

Die IGA-Policy sollte schriftlich festgehalten werden

Viele Bereiche rund um Identity Lifecycle Management-Prozesse erfordern das Treffen von Entscheidungen außerhalb des IGA-Systems. Dazu gehört auch die Beantwortung der Fragen, wie lange Externe vor einer Rezertifizierung Zugriff auf Anwendungen haben sollten, wie nicht-personenbezogene technische Identitäten zu handhaben sind und welche Übergangsphasen man bei der Übergabe des Zugriffs von einem Mitarbeiter zum nächsten definiert. Zur Vermeidung spontaner Policy-Entscheidungen, die Governance-Verstöße nach sich ziehen könnten, wird empfohlen, eine formelle schriftliche Policy einzuführen. Ohne schriftliche Policy könnte die Gewährung von Zugriff einen Verstoß darstellen. Außerdem könnte es zu mangelnder Kohärenz zwischen verschiedenen Abteilungen kommen. Oder zu Zeitvergeudung durch Diskussionen über jeden Einzelfall.

?

Fragen, die man sich zum Identity Lifecycle Management stellen sollte

- Aus welchen Quellen kommen meine Stammdaten?
- Wie sollten Stammdaten zur Verfügung gestellt werden?
- Bestehen Regeln zur Erstellung eindeutiger Identifier?
- Sind zur Abwicklung der Prozesse Governance-Verfahren vorhanden?
- Sind die aktuellen Standards dokumentiert und erfüllen sie die aktuellen und zukünftigen rechtlichen Anforderungen?

Zusammenfassung

Das Identity Lifecycle Management umfasst sämtliche Prozesse eines Identity Lifecycle: Vom Eintritt als Mitarbeiter oder Externer bis hin zur Beendigung der Zusammenarbeit mit dem Unternehmen. Dies umfasst sämtliche Schritte des gesamten Arbeitslebens einschließlich aller Namensänderungen, Elternzeiten, Aus- und Wiedereintritte in das Unternehmen etc.

In einer anpassungsfähigen Identity Lifecycle Management-Lösung lassen sich Business-Funktionen an veränderte geschäftliche Anforderungen anpassen. Dies umfasst auch Prozesse für die IT- und Business-Zusammenarbeit, Funktionstrennung (SoD) sowie branchenspezifische Rollen- und Policy-Modelle, die beliebige Levels bei Rollen, Rollentypen und Klassifikationen ermöglichen.

Moderne Lifecycle Management-Modelle integrieren verschiedenste Anwendungen und Systeme (wobei manche Teile der Identität in Anwendungen wie ERP, andere in Identity Stores wie Microsoft AD gemanagt werden) in ein logisches Geschäfts-Anwendungsmanagement und erleichtern dadurch das Onboarding von Anwendungen, Systemressourcen, Self-Service-Berechtigungsanträge und Governance Reporting.

Prozessbereich

Access Management

Die in IdentityPROCESS+ definierten Access Management-Prozesse ermöglichen Organisationen die Steuerung der Gewährung von Zugriffsrechten und stellen zugleich sicher, dass dabei nicht gegen Sicherheits- und Compliance-Policies wie z. B. die Funktionstrennung (SoD) verstoßen wird.

Wurden Identitäten von Identity Lifecycle Management Prozessen erstellt, erhalten neue oder Mitarbeiter, die in eine andere Abteilung wechseln,die Zugriffsrechte, die sie benötigen, um ihre täglichen Arbeitsaufgaben zu erledigen. Mit der Zeit kann es sein, dass sie die Rechte auf Zugriff zu einem System erweitern müssen, weil sie einer neuen Abteilung oder Region zugewiesen wurden oder weil sie befördert wurden und daher Zugriff auf weitere Funktionalitäten in bereits von ihnen genutzten Anwendungen benötigen. Ebenso kann es auch sein, dass im Zuge der Weiterentwicklung des Unternehmens neue Anwendungen eingeführt werden, auf die Mitarbeiter zugreifen müssen.

Bisher verwalteten die IT-Abteilungen Zugriffsrechte in Tabellen, die den Prozess auch gegenüber Auditoren dokumentierten. Der Haken an dieser traditionellen Vorgehensweise: Sie ist sehr zeitaufwändig, fehleranfällig und kann gegen interne Policies oder externe Bestimmungen verstoßen. Zu Audits herangezogene Unterlagen können fragmentiert vorliegen, da die Gründe, weshalb Zugriff gewährt wird, nicht sauber protokolliert werden. Außerdem sammeln Mitarbeiter im Laufe der Zeit immer mehr Zugriffsrechte an, weil diese nicht widerrufen werden, wenn sie in eine andere Abteilung wechseln oder die Arbeit an einem Projekt abschließen.

Die in IdentityPROCESS+ definierten Access Management-Prozesse ermöglichen Organisationen, die Steuerung der Gewährung von Zugriffsrechten und stellen zugleich sicher, dass dabei nicht gegen Sicherheits- und Compliance-Policies wie z. B. Funktionstrennung (SoD) verstoßen wird. Darüber hinaus bedeutet die Definition von Self-Service Berechtigungsanträgen, dass die Prozesse den Arbeitsaufwand der IT-Abteilung senken, da Prozesse rund um die Gewährung von Zugriffsrechten automatisiert und delegiert werden. Die Prozesse beschreiben auch, wie man Enddaten festlegt, um sicherzustellen, dass einem Benutzer der Zugriff verweigert wird, wenn ein Zugriff nicht mehr erforderlich ist.

Das Access Management besteht aus drei Prozessen (einschließlich Beantragung von Zugriffsrechten) und beschreibt ganz einfach, wie Benutzer Zugriff beantragen, bewerten und handhaben können – dies umfasst auch Prozesse für die Genehmigung und den Entzug von Zugriffsrechten als auch das Delegieren von Zugriffsrechten sowie schließlich auch die Provisionierungsgruppe, die untersucht, wie Zugriff zu seltener verwendeten, nicht mit dem IGA-System verbundenen Systemen gewährt werden kann.

Der Prozessbereich „Access Management“ umfasst die folgenden Prozesse:

Beantragung von Zugriffsrechten

- Berechtigungsantrag

Auswertung und Genehmigung

- Gewährung von Zugriffsrechten
- Delegation von Rechten
- Zugriff entziehen

Provisionierung

- Manuelle Provisionierung

Prozess

Beantragung von Zugriffsrechten

Automatisiert Berechtigungsanträge und lässt Endbenutzern die benötigten Angaben machen, damit der Zugriff schnell und ohne Verstöße gegen Sicherheits- und Compliance-Bestimmungen möglich wird.

BERECHTIGUNGSANTRÄGE

Im Laufe der Zeit müssen Benutzer zusätzliche Systemzugriffe beantragen, wenn sich ihre Aufgaben im Unternehmen ausweiten. Wichtig dabei: dass ihnen Zugriff im richtigen Umfang gewährt wird und die Gründe für Audit-Zwecke korrekt dokumentiert werden.

Prozessbeschreibung

Bei Beginn der Beantragung von Rechten wird der Benutzer aufgefordert, den geschäftlichen Grund für die neuen Zugriffsrechte anzugeben. Dann löst der Prozess die Genehmigung des Berechtigungsantragsprozesses aus, bei dem der Manager den Antrag entweder genehmigt oder ablehnt. Bei Genehmigung wird der Zugriff automatisch bereitgestellt und der Benutzer erhält den neuen Zugriff. Anträge können auch im Namen anderer gestellt werden. Dadurch kann ein Manager auch Zugriff für einen Externen oder Mitarbeiter beantragen, der nicht mit dem System vertraut ist.

Best-Practice-IGA-System-Funktionalität

Der Benutzer stellt den Antrag auf Zugriff direkt im IGA-System und kann diesen nur absenden, wenn er auch einen geschäftlichen Grund genannt sowie Angaben zum Business-Kontext (Abteilung, Projekt, Kostenstelle) gemacht hat. Bei Übermittlung wird der Genehmigungsprozess für den Berechtigungsantrag eingeleitet. Eine Prüfung auf Funktionstrennung erfolgt automatisch, um sicherzustellen, dass der neue Zugriff für den Benutzer keine riskante Zugriffskombination mit sich bringt. Für jede angefragte Ressourcenaufgabe wird ein Genehmigungsprotokoll erstellt. So haben die Genehmigenden Einblick in die Gründe für die Genehmigung.

Für jede beantragte Berechtigungszuweisung werden Aufzeichnungen zum Genehmigungsverlauf geführt. Dieser Verlauf ist für die Genehmigenden im Verlauf der Prozesse sichtbar und lässt sie mitverfolgen, wer den Antrag zuvor aus welchen Gründen genehmigt hat.

Technischer Prozessablauf

1. Der Benutzer loggt sich ein und beginnt den Berechtigungsantrags-Workflow durch Eintragen von Details in das Antragsformular wie z.B.: die Identität, für die der Antrag gestellt wird, Grund für den Antrag sowie geschäftlicher Kontext.
2. Der Benutzer stellt Anträge mit Blick auf seine eigene Identität oder Identitäten, die von ihm gemanagt werden bzw. ihm gehören. Optional kann der Benutzer auch ein Benutzerkonto angeben, für das die Ressource beantragt wird und eine Gültigkeitsdauer für den beantragten Zugriff angeben.
3. Der Benutzer sucht nach Rollen und Ressourcen, die er anfragen kann. Verlangt eine Ressource vom Benutzer die Auswahl oder Angabe eines Attributs, wird dieses ausgewählt.

Prozess

Auswerten und Agieren

Verwaltet das Routing von Self-Service Berechtigungsanträgen zur Genehmigung, automatisiert die Terminierung nicht mehr benötigter Zugriffsrechte und übernimmt das Delegieren von Zugriffsrechten, wenn Mitarbeiter das Unternehmen verlassen oder diesem längere Zeit fernbleiben.

GEWÄHRUNG VON ZUGRIFFSRECHTEN

Vor Genehmigung eines Berechtigungsantrages ist dieser zu überprüfen, um sicherzustellen, dass er keinen Verstoß gegen Konflikt-Policies wie z. B. Funktionstrennung (SoD) auslöst. Dann erfolgt die Gewährung oder Ablehnung durch den Eigentümer der Fachanwendung.

Prozessbeschreibung

Der Prozess der Genehmigung von Zugriffsrechten steht in enger Verbindung mit der Beantragung von Rechten und beginnt, wenn ein Benutzer einen Zugriff beantragt.

Der Prozess umfasst vier Aufgaben:

1. Der Antrag geht bei der zuständigen genehmigenden Person – in der Regel dem Eigentümer der Fachanwendung oder Manager – ein, der nach Erhalt dann den Zugriff erlauben oder ablehnen kann.
2. Eine Gegenprüfung mit der Policy zur Funktionstrennung (SoD) wird ebenfalls durchgeführt, um sicherzustellen, dass die Gewährung des Zugriffs keine Aktionen ermöglicht, die den Policies des Unternehmens zuwiderlaufen.
3. Führung eines Protokolls mit Verlaufsaufzeichnungen über Genehmigtes, Zeit und Begründungen. Das Protokoll hilft dem Genehmigenden, die Eignung von Zugriffsanträgen im Kontext des zuvor Gewährten bzw. Abgelehnten zu beurteilen.
4. Der Zugriff wird gewährt, wenn der Antrag genehmigt wird und gegen keine bestehenden Business-Policies verstößt.

Best-Practice-IGA-System-Funktionalität

Nach Durchführung des Prozesses zur Beantragung von Rechten erstellt das IGA-System automatisch eine Aufgabe für die zuständige genehmigende Person. Ein SoD-Policy-Check und andere konfigurierte Konflikt-Prozess-Prüfungen werden durchgeführt und das Informationsprotokoll wird mit relevanten Daten aktualisiert. Das IGA-System legt fest, was bereitzustellen ist, um die Anfrage zufriedenstellend bearbeiten zu können und übermittelt diese Angaben zur Provisionierung. Für jede beantragte Berechtigungszuweisung werden Aufzeichnungen zum Genehmigungsverlauf geführt. Dieser Verlauf ist für die Genehmigenden im Verlauf der Prozesse sichtbar und lässt sie mitverfolgen, wer den Antrag zuvor aus welchen Gründen genehmigt hat.

Technischer Prozessablauf

1. Der eingehende Antrag auf Gewährung eines Zugriffs wird entweder genehmigt oder abgelehnt.
2. Rollen- und Policy-Berechnungen werden einschließlich einer Bewertung eventueller SoD-Verstöße ausgelöst.
3. Die Provisionierung im Zielsystem wird durchgeführt.

DELEGIEREN VON ZUGRIFF

Gelegentlich kann es erforderlich sein, dass ein Benutzer seine Zugriffsrechte an einen Kollegen delegiert, z. B. während er im Urlaub ist. Ein Manager kann seine Zugriffsrechte über einen längeren Zeitraum an einen persönlichen Assistenten oder Projektkoordinator delegieren. Ein solches Delegieren des Zugriffs ist zeitlich beschränkt; deshalb bleiben die Gesamt-Zugriffsrechte auch bei der delegierenden Person, wodurch auch kontinuierliche Compliance gesichert wird.

Prozessbeschreibung

Der Prozess des Delegierens von Rechten gestattet Benutzern die vorübergehende Zuweisung von Rechten an andere Benutzer. Der Prozess enthält mehrere Verfahrenselemente, die sicherstellen, dass Organisationen im Zuge eines solchen Transfers keinen unnötigen Sicherheitsrisiken ausgesetzt werden.

Eines der Verfahren stellt sicher, dass die delegierten Zugriffsrechte in dem Moment, wo sie der delegierenden Person entzogen werden, sofort auch der Person entzogen werden, auf die sie delegiert wurden. Ein anderes, dass Segregation of Duty (SoD)-Policies beim Delegieren von Rechten auf schädliche Kombinationen überprüft werden. Und schließlich ist es sowohl möglich als auch Best Practice, das Delegieren auf einen bestimmten Zeitraum zu beschränken wie z. B. auf die Zeit, in der die delegierende Person im Urlaub ist oder für die ungefähre Dauer z. B. einer Elternzeit. Dies sorgt dafür, dass der erweiterte Zugriffslevel nicht in Vergessenheit gerät und der User im Laufe der Zeit keine übermäßigen Zugriffsrechte anhäuft.

Best-Practice-IGA-System-Funktionalität

Beim Delegieren von Zugriffsrechten im IGA-System wählt die delegierende Person die zu delegierenden Zugriffsrechte, den Benutzer, auf den delegiert werden soll sowie den Gültigkeitszeitraum aus. Das System analysiert automatisch, ob es zu Verstößen gegen Policies kommt und lehnt den Antrag dann entweder ab oder stellt den Zugriff bereit.

Technischer Prozessablauf

1. Der Benutzer wählt eine Identität aus, auf die er Zugriffsrechte delegieren will.
2. Der Benutzer wählt die zu delegierenden Zugriffsrechte aus und füllt die Felder „Gültig ab“ und „Gültig bis“ aus.
3. Der Benutzer versendet den Antrag.
4. Die für die Identität geltenden Rollen und Policies werden überprüft.
5. Die delegierten Zugriffsrechte werden gewährt.

ZUGRIFF ENTZIEHEN

Zu Wahrung hoher Compliance- und Sicherheitsstandards müssen Organisationen bei Beendigung der Tätigkeit von Mitarbeitern bzw. Externen bzw. deren Wechsel in andere Abteilungen oder Beförderungen nicht mehr benötigte Zugriffsrechte terminieren.

Prozessbeschreibung

Der Prozess zum Entziehen von Zugriffsrechten stellt sicher, dass Zugriffsrechte entzogen werden, wenn diese nicht mehr gebraucht werden; er wird in folgenden Situation ausgelöst:

1. Eine Identität deaktiviert ihren eigenen direkten Zugriff.
2. Ein Manager deaktiviert den direkten Zugriff für einen ihm direkt unterstellten Mitarbeiter.
3. Ein System- oder Ressourcen-Eigentümer deaktiviert den direkten Zugriff auf ein von ihm gemanagtes System oder eine Ressource.
4. Ein zuvor gewährtes Zugriffsrecht erreicht das Ablaufdatum.
5. Es liegt stets im Ermessen eines Datenverantwortlichen, den direkten Zugriff auf eine beliebige Identität zu deaktivieren.

Best-Practice-IGA-System-Funktionalität

Ein Benutzer oder Manager loggt sich im IGA-System ein und entscheidet sich für Terminierung des Zugriffs. Nach Auswahl und Bestätigung wird der Zugriff im Zielsystem deaktiviert und deprovisioniert. Wird der Prozess durch ein Ablaufdatum ausgelöst, werden dieselben Schritte automatisch durchgeführt.

Technischer Prozessablauf

1. Der Benutzer loggt sich in die IGA-Lösung ein und öffnet die Übersicht für die Identität, für die er den Zugriff deaktivieren will.
2. Der Benutzer wählt den gewünschten Zugriff aus und bestätigt diesen.
3. Der Zugriff wird deprovisioniert.

Prozess

Provisionierung

Verwaltet die Aufzeichnung und Protokollierung von Zugriffsrechten für im IGA-System nicht automatisierbare Anwendungen.

MANUELLE PROVISIONIERUNG

Die Integration sämtlicher Anwendungen einer Organisation in das IGA-System ist möglicherweise weder möglich noch erstrebenswert – aus Compliance-Gründen ist es dennoch erforderlich, Zugriff zu ermöglichen und Aktivitäten zu protokollieren.

Prozessbeschreibung

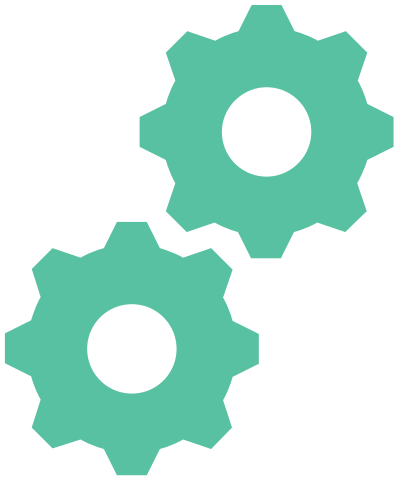
Ein zentraler Vorteil eines IGA-Systems: die Automatisierung der Provisionierung oder Zuweisung von Zugriffsrechten für einen Benutzer in der anvisierten Fachanwendung. Der manuelle Provisionierungsprozess stellt sicher, dass man auch an Systeme provisionieren kann, die nicht mit dem IGA-System verbunden sind und dennoch Aktivitäten im IGA-System überprüfen und protokollieren kann und so Auditing- und Compliance-Vorgaben erfüllt. Die Anfrage erfolgt im IGA-System. Die provisionierende Person, der Benutzer oder die Benutzergruppe, der/die für die Verarbeitung der Anfrage zuständig ist, erhält dann eine Benachrichtigung zur manuellen Durchführung der Aufgabe. Sowohl der Antragsteller als auch der Bereitstellende gibt relevante Informationen in das IGA-System ein.

Best-Practice-IGA-System-Funktionalität

Der Antragsteller stellt seine Anfrage direkt im IGA-System; der Bereitstellende erhält eine manuelle Provisionierungs-Aufgabe. Der Bereitstellende führt manuell die Aufgaben zur Erstellung der Zuweisung zwischen Identität und Ressource im Zielsystem durch und bestätigt dann im IGA-System den Abschluss der Aufgabe.

Technischer Prozessablauf

1. Das IGA-System stellt fest, dass zur Zuweisung eines Zugriffs eine manuelle Provisionierung erforderlich ist
2. Das IGA-System erstellt eine manuelle Provisionierungsaufgabe
3. Eine E-Mail-Benachrichtigung wird an alle für manuelle Provisionierung zuständigen Personen versandt, die manuell auf das Zielsystem zugreifen und Zugriff dazu gewähren
4. Die manuelle Provisionierung wird von der provisionierenden Person in der IGA-Lösung bestätigt
5. Das IGA-System protokolliert diesen Vorgang



Access Management

Die erfolgreiche Durchführung von Access Management-Prozessen beruht auf einer Kombination, bei der Endbenutzer Zugriffsrechte beantragen und deren Vorgesetzte diese Anträge effizient genehmigen oder ablehnen können.

PROZESS-STAKEHOLDERS

Access Management-Prozesse haben überwiegend den Endbenutzer im Blick. Das bedeutet, dass alle mit diesen Prozessen verknüpften Aufgaben erst nach der Implementierung durchzuführen sind und nur Endbenutzer und deren Vorgesetzte daran mitwirken. Die Personalabteilung, das IGA-Team sowie die Eigentümer von Anwendungen sind nicht direkt an diesen Prozessen beteiligt.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
IGA-Team	Keine	Keine	Keine	Prozessablauf überprüfen. Vorgehen in Ausnahmefällen, wenn keine genehmigenden Personen verfügbar sind.
Line Managers	Vorgesetzte sind am Berechtigungsantragsprozess beteiligt, da sie Anträge entweder genehmigen oder ablehnen. Vorgesetzte können bei Bedarf auch ihnen direkt unterstellten Mitarbeitern den Zugriff entziehen.	Manager sind in der Regel in der besten Position, um die Zugriffsrechte von ihnen direkt unterstellten Mitarbeitern zu genehmigen, abzulehnen oder zu deaktivieren, weil sie die geschäftliche Situation und die Verwendung der damit verbundenen Anwendungen genau kennen.	Keine	1) Analysieren von Berechtigungsanträgen, wenn eine Aufgabe dem Vorgesetzten zugewiesen wird und Genehmigung bzw. Ablehnung auf Grundlage der verfügbaren Informationen. 2) Entfernen des Zugriffs von direkt unterstellten Mitarbeitern, wenn diese keinen direkten Zugriff mehr auf bestimmte Geschäftssysteme benötigen.
End Users	Endbenutzer beantragen neue Zugriffsrechte, wenn sie der Meinung sind, dass sie zur Durchführung ihrer Aufgaben Zugriff auf neue Anwendungen brauchen. Endbenutzer können sich auch für ein Delegieren ihrer Zugriffsrechte entscheiden, wenn sie eine bestimmte Zeit lang nicht im Büro tätig sind.	Endbenutzer brauchen die Möglichkeit, den Zugriff zu neuen Systemen zu beantragen und ihre bestehenden Zugriffsrechte zu delegieren.	Keine	1) Einsatz des Berechtigungsantragsprozesses, wenn sie auf neue Anwendungen zugreifen müssen. 2) Einsatz des Prozesses zum Delegieren von Zugriffen, wenn sie ihre Zugriffsrechte vorübergehend einem anderen Benutzer übertragen wollen.
Business System Owners	Eigentümer von Anwendungen müssen Zugriffsanträge genehmigen.	Sie sind verantwortlich für die Sicherheit ihrer Systeme und müssen daher auch Zugriffsrechte für Benutzer genehmigen.	Keine	Kontinuierliches Reagieren auf Anträge zu Zugriffsrechten.

Wichtige Best Practices

Empfehlungen

Nachfolgend eine Reihe von Best-Practice-Empfehlungen, die bei der Implementierung von Access-Prozessen in IdentityPROCESS+ bedacht werden sollten.

ZUGRIFFSRECHTE

Festlegen, ob manche Benutzer auch für andere Personen Zugriffsrechte beantragen können

Für bestimmte Benutzer kann es angezeigt sein, im Namen anderer Mitarbeiter Zugriffsrechte zu beantragen. So kann z. B. eine Organisation Managern für deren direkt unterstellte Mitarbeiter den Zugriff zu bestimmten Anwendungen gestatten; oder persönliche Assistenten müssen Zugriff für ihre Manager beantragen.

Gestattet man bestimmten Benutzern den Zugriff im Namen von anderen, trägt dies zur Steigerung der Gesamteffizienz bei und beschleunigt die betrieblichen Abläufe. Es sind aber auch Maßnahmen zur Vermeidung von Missbrauch zu treffen. Die Umstände, unter denen es Personen gestattet ist, Zugriff im Namen anderer zu beantragen, sind in einem schriftlichen IGA-Policy-Dokument niederzulegen.

Festlegen, wer Einzelpersonen Zugriffsrechte entziehen darf

Der Entzug von Zugriffsrechten könnte dazu führen, dass Mitarbeiter ihre täglichen Aufgaben nicht mehr wahrnehmen können. Es kann aber auch Situationen geben, wo Zugriffsrechte entzogen werden müssen, z. B. bei Verdacht auf Sicherheitsverstöße, Verstößen gegen die Funktionstrennung (SoD) oder wenn die Organisation den Verdacht hat, dass der Benutzer ihre Verwendungsregeln für Informationstechnologie missbräuchlich handhabt.

Organisationen müssen sicherstellen, dass Mitarbeiter mit Befugnis zum Entzug von Zugriffsrechten die geschäftlichen Implikationen einer solchen Handlung verstehen. Die Umstände, unter denen es Personen gestattet ist, Zugriff zu entziehen, sind in einem schriftlichen IGA-Policy-Dokument niederzulegen.

GENEHMIGUNGEN

Feststellen, ob eine genehmigende Person Anträge ändern kann

Für eine genehmigende Person kann es angebracht sein, einen Antrag zu ändern. Beispielsweise, wenn sie den Eindruck hat, dass das „Gültig bis-"Datum nicht die Compliance-Vorgaben erfüllt. Das Zulassen von Änderungen beschleunigt den Genehmigungsprozess, erfordert jedoch auch sorgfältiges Management, um sicherzustellen, dass die Änderungen im Einklang mit den Richtlinien des Unternehmens stehen. Sind Änderungen gestattet, sollte der Prozess in einem schriftlichen IGA-Policy-Dokument erklärt werden.

Entscheiden, ob für die Gewährung von Zugriffsrechten ein implizites oder explizites Modell Anwendung finden soll

Zur Steigerung der Effizienz gewähren manche Organisationen Benutzern auf Grundlage bestimmter vordefinierter Regeln ein bestimmtes Level an Zugriffsrechten – oftmals als „Birthrights" bezeichnet.
Andere Organisationen wiederum scheuen eher das Risiko und fordern daher für jeden Fall einen ausdrücklichen Genehmigungsschritt.

Beide Möglichkeiten haben Vor- und Nachteile – welches Vorgehen für sie am besten ist, muss jede Organisation selbst entscheiden. Das implizite Gewähren von Zugriff ist effizient, weil dafür kein Manager grundlegende Zugriffsrechte gestatten muss. Vielmehr erhalten alle neuen Mitarbeiter diese Rechte auf Basis ihrer grundlegenden Jobanforderungen (z. B. Email, Access Directory und Spesenanwendung). Zum impliziten Gewähren von Zugriffen müssen jedoch Rollendefinitionen vorhanden sein.

Für eine explizite Genehmigung sind weniger vorbereitende Schritte erforderlich. Daher müssen im Vorfeld keine Rollen definiert werden; für jeden neuen Mitarbeiter sind jedoch Zugriffsrechte festzulegen.

Daher wird empfohlen, dass Organisationen, wo immer möglich, vordefinierte Regeln zur Zuweisung von Zugriffsrechten anwenden, da dies den Arbeitsaufwand der genehmigenden Manager und den Zeitaufwand bei der Gewährung von Zugriffsrechten für Benutzer reduziert.

Gewährung von Zugriffsrechten über Vorgesetzte
Es ist wichtig, dass Vorgesetzte die Zugriffsrechte kennen, über die ihre direkt unterstellten Mitarbeiter verfügen. Deshalb die Empfehlung, alle Genehmigungsprozesse über Vorgesetzte abzuwickeln. Gegebenenfalls könnten Genehmigungen auch für Daten- und Anwendungseigentümer benötigt werden. Dies sollte jedoch besonderen Anwendungen vorbehalten bleiben, da hier zusätzliche Schritte zu durchlaufen sind, die den Genehmigungsprozess verlangsamen.

COMPLIANCE

Gültigkeitsperioden für externe Benutzer
Zur Verbesserung der Compliance sollten externe Benutzer wie Lieferanten und externe Geschäftspartner je nach Sensibilität der Ressource Zugriff nur über begrenzte Zeiträume (z. B. drei oder sechs Monate lang) erhalten. Das Level des Zugriffs sollte ihren Aufgaben angemessen sein. Dadurch muss der genehmigende Manager zwar regelmäßig eine Zusatzaufgabe erledigen, doch es schafft auch eine Compliance, durch die kurzfristig für das Unternehmen Tätige nach Beendigung dieser Tätigkeit keinen Zugriff mehr auf Unternehmensdaten haben.

Steigerung der Compliance durch Ressourcenqualifikation
Zur Steigerung der Effizienz beim Managen von Compliance-Anforderungen wird empfohlen, Ressourcen mit Tags zu klassifizieren. Klassifizierung verschiedener Ressourcen auf Basis der Daten, die diese verarbeiten, macht es leichter, festzustellen, wie diese zu managen sind und damit auch, welche Zugriffs-Policies aufgrund bestehender gesetzlicher Vorgaben wie der DSGVO umzusetzen sind.

VERSCHIEDENES

Berücksichtigung des Faktors Business Continuity sicherustellen
Organisationen müssen ermitteln, ob es geschäftskritische Anwendungen gibt, die das Unternehmen dringend benötigt und bei denen die Gewährung eines Zugriffsrechts an nur eine Person Probleme in punkto Business Continuity mit sich bringen könnte. So stünde eine Organisation beispielsweise vor einem Problem, wenn der einzige Mitarbeiter, der Zugriff zur Server-Backup-Software hat, gerade nicht im Büro ist, wenn Daten wiederhergestellt werden müssen.

Benachrichtigungen sparsam einsetzen
Da Manager häufig zahlreiche E-Mail-Benachrichtigungen erhalten, ist es nicht unwahrscheinlich, dass sie wichtige Updates übersehen und nicht durchführen. Es wird empfohlen, dass Organisationen prüfen, ob Benutzer wirklich über jedes Event im IGA-System informiert werden müssen. Stattdessen sollten Organisationen erwägen, Vorgesetzte zu bitten, sich im IGA-System einzuloggen und dort ihre Tasklisten regelmäßig abzuarbeiten. Dies stellt sicher, dass keine wichtigen Aufgaben übersehen werden.

?

Fragen, die man sich zum Access Management stellen sollte

- Wer kann Zugangsrechte im Namen anderer Benutzer beantragen?
- Wer ist für die Löschung von Zugangsrechten zuständig?
- Sollte eine genehmigende Person zur Änderung eines Berechtigungsantrags befugt sein?
- Sollten Zugangsrechte implizit gewährt werden oder sollten explizite Genehmigung erforderlich sein?

Zusammenfassung

Access Management umfasst alle Prozesse zum Managen von Benutzeranfragen – vom Antrag eines Benutzers auf Zugriff zu einem System (der dann vom Manager oder Eigentümer der Fachanwendung genehmigt wird) bis hin zur Terminierung von Zugriffsrechten nach Beendigung der Zusammenarbeit mit dem Unternehmen.

Das Access Management ermöglicht auch das kurz- oder langfristige Delegieren von Zugriffsrechten an andere Mitarbeiter.

Eine ausgereifte IGA-Lösung lässt Benutzer den Zugriff auf benötigte Anwendungen oder Anwendungen beantragen, leitet solche Anfragen automatisch an zuständige genehmigende Personen weiter und führt Überprüfungen durch, um sicherzustellen, dass jeder gewährte Zugriff weder gegen die Funktionstrennung (SoD) noch gegen andere Regelwerke verstößt.

Prozessbereich

Business Alignment

Nach vollständiger Implementierung handhabt ein IGA-System alle mit einer Organisation verbundenen Identitäten. In manchen Organisationen können dies Tausende von Identitäten sein, bestehend aus Mitarbeitern, technischen Identities, Externen, Geräten und Endbenutzern.

Würden all diese Identitäten einzeln und fallweise gemanagt, wäre die Aufgabe sehr zeitraubend und äußerst komplex. Stellen Sie sich dazu einfach vor, wie komplex sich dann der Eintritt von 10 neuen Mitarbeitern pro Monat im gesamten Unternehmen gestalten würde. Sie würden in verschiedene Abteilungen eintreten und manche könnten zu verschiedenen Teams und Projekten gehören.
Da jedoch viele Mitarbeiter zur Durchführung ihrer täglichen Aufgaben die gleichen oder ähnliche Zugriffsrechte brauchen, kann man die Gewährung von Zugriffen beträchtlich vereinfachen, wenn man Mitarbeiter nach deren Aufgaben (Rollen) und Einsatzorten (Kontexte) ordnet.

Warum Business Alignment wichtig ist:

1. Zur Vereinfachung von IGA-Prozessen für nicht-technische Benutzer.
2. Um die dauerhafte Gewährung von Zugängen für Mitarbeiter mit gleicher Position oder geschäftlicher Situation effizient zu gestalten.
3. Zum effektiven Management feingranularer Definitionen von Zugangsbeschränkungen.

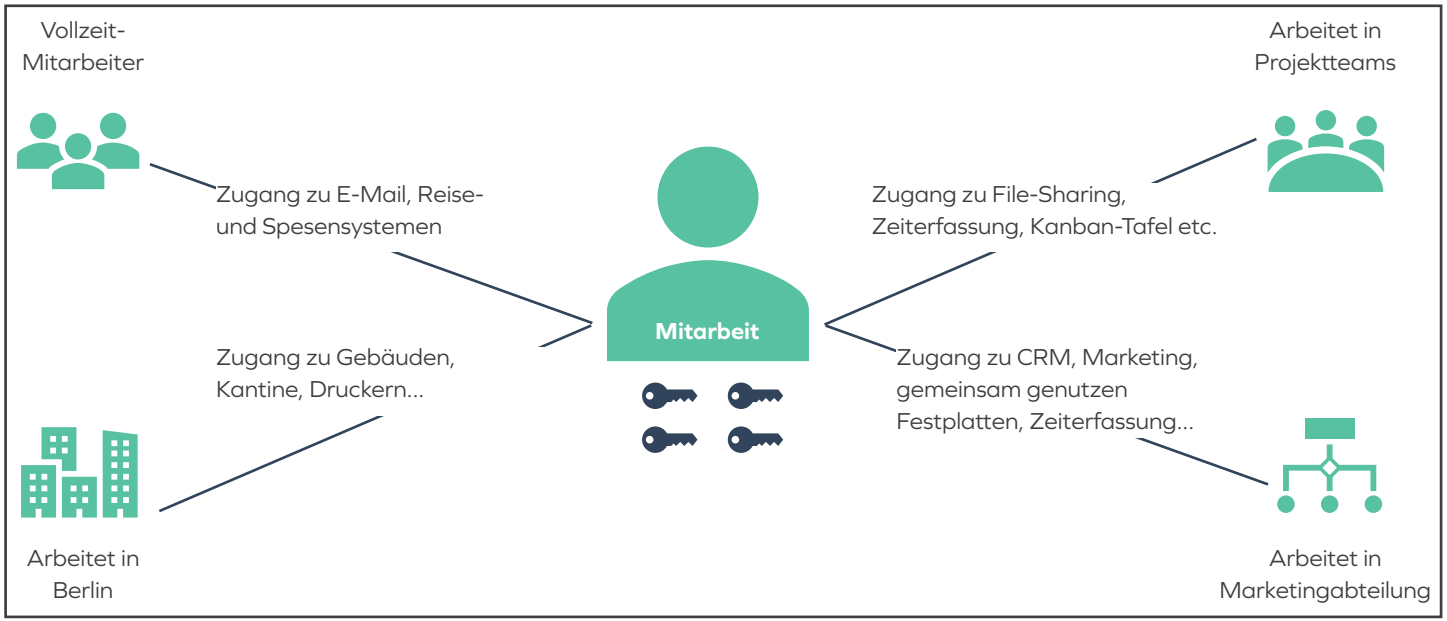


Abb. 5: Erstellen von an das Unternehmen angepassten Rollen, Kontexten und Policies vereinfacht Ihre Identity- und Access Governance.

Business Alignment

Der Prozessbereich Business Alignment senkt die Komplexität desOnboarding und Managens von Mitarbeiterzugängen durch Anwendung von Rollen, Policies und Kontexten mit vordefinierten Zugriffsrechten, denen Mitarbeiter zugewiesen werden können. Die festgelegten Policies und Kontexte können so gestaltet werden, dass sie die Business-Struktur in der IGA-Lösung präzise abbilden.

Insgesamt gestattet dies Organisationen eine Optimierung von deren IGA-Einsätzen und die Realisierung von Quick Wins im Lauf des Projekts durch erhöhte Benutzer-Akzeptanz. Die drei Prozesse werden im Folgenden näher erklärt.

Managen von Rollen
Business Alignment beginnt beim Definieren von Rollen, also Listen von Zugriffsvoraussetzungen für Benutzer mit den gleichen oder sehr ähnlichen Jobs. Haben in einer Organisation mehrere Mitarbeiter dieselbe Rolle inne – wie z. B. Sales Manager und Helpdesk-Mitarbeiter – erleichtert das Definieren von Rollen deren Start im Unternehmen erheblich.

Managen von Policies
Business-Alignment-Prozesse ermöglichen die Festlegung von Assignment-Policies, die bei Erfüllung bestimmter Kriterien einer Person automatisch bestimmte Rechte gewähren. Dies könnte beispielsweise der Zugriff auf gemeinsam genutzte Dateien für alle Mitarbeiter einer Abteilung sein. Oder der Zugriff zu Druckern für alle Mitarbeiter im 3. Stock.

Zuweisungs-Regeln lassen sich mit bestimmten Start- und Enddaten verknüpfen, um den Zugriff zu beschränken; so bleibt das Unternehmen sicher und hält bestehende Regeln ein.

Managen von Kontexten
Wie Rollen machen auch Kontexte das Managen von Usern mit ähnlichen Zugriffsanforderungen einfacher, da diese als eine Einheit verwaltet werden können. Im Unterschied zu Rollen haben die gemanagten Personen jedoch nicht unbedingt die gleiche Jobfunktion, sondern gemeinsame geschäftliche Interessen. So können beispielsweise mehrere Mitarbeiter, die an einer Fertigungslinie arbeiten, Zugriff zur selben Produktionsdatenbank brauchen – und dies, obwohl sie verschiedene Rollen haben. In diesem Fall wären alle verschiedenen Jobfunktionen Bestandteil des Kontexts „Produktionsmitarbeiter".

Kontexte ermöglichen Unternehmen die Modellierung und Verwaltung komplexer Situationen wie z. B. Matrix-Management-Strukturen oder Organisationen, wo Mitarbeiter in Verbindung mit mehreren Abteilungen stehen.

Der Prozessbereich Business Alignment umfasst die folgenden Prozesse:

Rolle managen

- Rollen erstellen, ändern oder löschen

Policy managen

- Zuweisungs-Regeln erstellen, ändern oder löschen
- Ausschlussregeln erstellen, ändern oder löschen

Management-Kontext

- Kontextzuweisungen erstellen, ändern, löschen, beantragen und genehmigen, verlängern und entfernen

Prozess

Rolle managen

Ermöglicht Organisationen eine schnelle und leichte Zuweisung einer Reihe von Zugriffsrechten an neue Benutzer mit denselben Positionen.

ROLLEN ERSTELLEN, ÄNDERN ODER LÖSCHEN

Das manuelle Zuweisen von Zugriffsrechten durch Personen ist zeitraubend, monoton und fehleranfällig. Durch Erstellen einer Reihe von Zugriffsrechten („Rollen") für eine gemeinsame Jobfunktion und deren vielfache Anwendung steigern Organisationen ihre Effizienz und senken die Fehlerwahrscheinlichkeit. Dies schafft erhöhte Sicherheit und senkt Compliance-Risiken.

Prozessbeschreibung

Die Manage-Rolle-Prozesse, bei der Rollen erstellt, geändert und deaktiviert werden, ermöglichen Administratoren das Management von Beschreibungen der Zugriffsvoraussetzungen für User mit den gleichen oder sehr ähnlichen Aufgaben. Tritt ein neuer Mitarbeiter in das Unternehmen ein und wird ihm eine Rolle zugewiesen, erhält er automatisch Zugriff auf alle Systeme, die er zur Durchführung seiner Aufgaben braucht. So sollte z. B. das gesamte Sales-Personal Zugriff zum CRM- und E-Mail-System des Unternehmens sowie zu dessen Spesen- und Reiseanwendung haben. Anstatt also die Zugriffsrechte einzeln zu vergeben, werden alle auf einmal zugewiesen, wenn ein neuer Mitarbeiter ins Unternehmen kommt.

Darüber hinaus können Rollen im Laufe der Zeit geändert werden, um sich an veränderte geschäftliche Anforderungen anzupassen wie z. B. an die Einführung neuer Anwendungen für bestimmte Jobs. Falls hier kein Bedarf mehr besteht, ist auch eine Terminierung möglich.

Best-Practice-IGA-System-Funktionalität

Zugriffsanforderungen, die zur Erfüllung der geschäftlichen Anforderungen der jeweiligen Jobfunktion nötig sind, werden mithilfe des neuen Rollen-Prozesses zusammengestellt. Rollen werden definiert, um Organisationsstrukturen, Businessstandorte und -prozesse oder Kontrollverfahren abzugleichen. Ihre Definition erfolgt im Einvernehmen mit geltendem Recht, regulatorischen Vorgaben und Sicherheitsregeln des Unternehmens. Nach erfolgter Definition werden die Rollen im IGA-System erstellt und den neuen Mitarbeitern auf Basis ihrer Jobbeschreibung im HR-System bei Eintritt ins Unternehmen bzw. Wechsel in einer neuen Position zugewiesen.

Bei Änderungen der geschäftlichen Anforderungen, für die die Rolle steht – z. B. die Einführung einer neuen Anwendung oder gesetzlichen Bestimmung – wird der „Modify Roles"-Prozess zur Aktualisierung der Rollendefinitionen verwendet. Ist die geschäftliche Notwendigkeit nicht mehr gegeben, wird der „Rolle beenden"-Prozess verwendet, um eine Rolle aus dem IGA-System zu löschen.

.

Technischer Prozessablauf

1. Ein Administrator erstellt Rollen auf Basis von Attributen wie z. B. Jobtiteln
2. Das IGA-System bestimmt, ob die einzelne Identität zur jeweiligen Rolle passt
3. Die entsprechenden Zugriffsrechte werden Identitäten passend zur betreffenden Rolle zur Verfügung gestellt

Prozess

Policy managen

Ermöglicht Organisationen eine schnelle und leichte Zuweisung einer Reihe von Zugriffsrechten an Benutzer, welche bestimmte Kriterien erfüllen sowie die Erstellung und das Management von Zugriffs-Ausschlussregeln.

ZUWEISUNGS-REGELN ERSTELLEN, ÄNDERN ODER LÖSCHEN

Die Einrichtung individueller, bestimmte Kriterien erfüllender Zugriffsrechte für Benutzer – wie z. B. Mitarbeiter einer Abteilung, die Zugriff zu vertraulichen Daten benötigen – ist ineffizient und potenziell fehleranfällig. Das Einrichten von Verfahren zur Automatisierung von Zuweisungen auf Policy-Basis steigert nicht nur die Effizienz, sondern senkt auch Sicherheit- und Compliance-Risiken durch Fehler bei der Zuweisung von Zugriffsrechten.

Prozessbeschreibung

Die Prozesse der Zuweisungs-Regeln – die u.a. die Regeln zur Erstellung, Änderung und Terminierung von Zuweisungen umfassen – managen die Policies und vergeben Zugriffsrechte an Benutzer, die bestimmte geschäftliche Kriterien erfüllen.

Im Gegensatz zu Rollen – die die Zuweisung von Zugriffsrechten über Jobtitel von Mitarbeitern vollziehen – beruhen Zuweisungs-Regeln auf dem Abgleich von passenden Identitätseigenschaften. Jede Identität, die in den Identitätsfilter fällt, der in der Assignment Policy festgelegt ist, erhält die damit verknüpften Zugriffsrechte. So würde beispielsweise ein in den USA tätiger Manager Zugriff zum Ausgabenmanagement des Unternehmens in USA erhalten und sein europäischer Kollege in gleicher Funktion Zugriff zum entsprechenden europäischen System.

Best-Practice-IGA-System-Funktionalität

Der Administrator setzt einen Identitätsfilter und erstellt eine neue Zuweisungs-Regel unter Verwendung des „Create New Assignment Policy"-Prozesses.
Alle die Filterkriterien erfüllenden Identitäten erhalten automatisch die in der Zuweisungs-Regel festgelegten Zugriffsrechte. Alle Änderungen der geschäftlichen Anforderungen lassen sich mit dem „Modify Assignment Policy"-Prozess durchführen.

Wird eine Zuweisungs-Regel mit dem „Terminate Assignment Policy"-Prozess deaktiviert, erlöschen auch alle damit verbundenen Zugriffsrechte. Wichtig ist, dass die Folgen des „Terminate Assignment Policy"-Prozesses vor einer Anwendung auf Endbenutzer genau geprüft werden, damit diesen nicht der Zugriff zu Anwendungen verwehrt wird, die von essenzieller Bedeutung für deren Tätigkeit sind.

Technischer Prozessablauf

1. Der Administrator erstellt die Zuweisungs-Regeln, die nicht nur Angaben zur Gültigkeit der Regeln, sondern auch über den Filter zur Definition von Identitäten, Kontexten und Kontotypen machen sollte. Die Zuweisungs-Regel enthält auch eine Liste von Ressourcen, die Identitäten zugewiesen werden sollten, zu denen der Filter passt
2. Eine Neuberechnung wird durchgeführt, um festzustellen, welchen Identitäten neue Rechte zugewiesen werden sollten
3. Neue Zugriffsrechte werden für die im Umfang inbegriffenen Identitäten gewährt

NEUE AUSSCHLUSSREGELN ERSTELLEN, ÄNDERN ODER LÖSCHEN

Organisationen müssen Mechanismen entwickeln, die verhindern, dass Endbenutzer Zugriff zu verschiedenen Systemen erhalten, der sie zur Durchführung betrügerischer Handlungen befähigen könnte. Ist dies nicht möglich, beispielsweise weil in der Abteilung nicht genügend Mitarbeiter vorhanden sind, um die Aufgaben aufzuteilen, muss eine umfassende KAudit Trail vorhanden sein. Dadurch lassen sich Risiken einer Genehmigung potenziell riskanter Kombinationen managen.

Prozessbeschreibung

Prozesse zum Management von Ausschlussregeln dienen der Erstellung, Änderung und Löschung von Ausschlussregeln wie z. B. der Funktionstrennung (SoD). Diese Policies werden immer dann überprüft, wenn ein Benutzer einen Self-Service Berechtigungsantrag stellt oder eine automatisierte Zuweisung erfolgt. Bei Verstoß gegen eine Policy wird der Zugriff nicht gewährt und der Vorgang an Vorgesetzte eskaliert, um eine geeignete Lösung festzulegen.

Best-Practice-IGA-System-Funktionalität

Der Prozess dient der Einrichtung von Zugriffsbeschränkungs-Kombinationen aufgrund von Geschäftsprozessen bzw. Ressourcen. Solche Einschränkungen verhindern, dass Zugriff zu Systemen gewährt wird, die für betrügerische Zwecke missbraucht werden könnten. Wird eine potenziell schädliche Zugriffskombination erkannt, werden die neuen Zugriffsrechte nicht gewährt und der Vorgang unter Anwendung eines vordefinierten Workflows eskaliert – so kann eine geeignete Lösung gefunden werden. Dies könnte dazu führen, dass ein Manager den Zugriff zu einem System verweigert oder gewährt und eine schlüssige Begründung für die manuelle Aufhebung der Beschränkung angibt. Die Regeln zum Verändern und Löschen von Ausschlüssen ändern bzw. heben die Ausschlussregeln auf und setzen dadurch aktuelle unternehmerische Anforderungen um.

Technischer Prozessablauf

1. Der Administrator legt Ausschlussregeln fest und definiert entweder einen schädlichen Geschäftsprozess oder eine Kombination aus solchen Ressourcen bzw. Attributen
2. Bei jeder Änderung der Zugriffsrechte einer Identität wird eine Neuberechnung durchgeführt
3. Liegt kein Verstoß gegen die Ausschlussregeln vor, wird der Zugriff gewährt
4. Liegt ein Verstoß gegen die Ausschlussregeln vor, wird der Zugriff verweigert und der Antrag zum Treffen weiterer Maßnahmen eskaliert

! BEST PRACTICE...

Definieren von Rollen und Ausschlussregeln eher nach geschäftlichen als nach technischen Gesichtspunkten – dadurch können die entsprechenden Geschäftsbereiche, wie z. B. die Finanz- oder Rechtsabteilung, bestimmen, ob die Anforderungen angemessen sind.

Prozess

Managen von Kontexten

Ermöglicht Organisationen eine schnelle und leichte Zuweisung einer Reihe von Zugriffsrechten an Benutzer in geschäftlichen Situation, die gleichen Zugriffsanforderungen haben.

KONTEXTZUWEISUNGEN ERSTELLEN, ÄNDERN, LÖSCHEN, BEANTRAGEN UND GENEHMIGEN, VERLÄNGERN UND ENTFERNEN

Wenn Benutzer aufgrund eines ähnlichen Tätigkeitsprofils gleiche Zugriffsanforderungen haben, können Administratoren dies bei der Zuweisung von Zugriffsrechten mithilfe von Kontexten als Einzelvorgang verwalten, anstatt die Vorgänge einzeln und ineffizient zu bearbeiten.

Prozessbeschreibung

„Manage-Context"-Prozesse umfassen die Erstellung, Änderung, Löschung, Beantragung, Genehmigung, Verlängerung und Entfernung von Kontexten und ermöglichen Administratoren eine zusammenfassende Bearbeitung von Benutzern mit den gleichen Zugriffsanforderungen. Diese logischen Gruppierungen können auf beliebigen Geschäftssituationen basieren: z. B. „alle Mitarbeiter an einem Standort" oder „alle Mitarbeiter an einem Kundenprojekt". Kontextgruppen erleichtern Organisationen das Management von Zugriffsrechten, da Änderungen dann auch auf Kontext-Ebene durchgeführt und an alle Mitglieder eines Kontextes weitergegeben werden können.

Im Vergleich zu Rollen – die auf Jobtiteln von Benutzern beruhen – sind Kontexte flexibler, da bei Bedarf beliebige Benutzer hinzugefügt werden können.

Best-Practice-IGA-System-Funktionalität

Administratoren können mit dem „Create New Context"-Prozess einen Kontext erstellen. Nach Erstellung kann ein Benutzer beantragen, Mitglied eines Kontexts zu werden. Wird der Antrag vom Kontext-Eigentümer genehmigt, erhält der Benutzer alle Zugriffsrechte. Diese Aktionen werden als Antrag durchgeführt und dienen der Genehmigung der Kontextzuweisung. Administratoren können vorhandene Datenfelder wie z. B. den Einsatzort eines Mitarbeiters verwenden oder eigene Felder erstellen und diese als Kontext einsetzen. Jeder Kontext kann einen oder mehrere Eigentümer haben, die für das Management der dem Kontext zugewiesenen Personen zuständig sind. Kontext-Eigentümer können bei Bedarf auch die Kontext- Zuordnung ändern oder löschen.

Technischer Prozessablauf

1. Ein Kontext-Eigentümer erstellt einen Business-Kontext
2. Ein Benutzer beantragt den Beitritt zu einem Business-Kontext
3. Der Kontext-Eigentümer erhält die Aufgabe zur Bewertung eines Beitrittsantrags
4. Der Antrag wird entweder genehmigt, wodurch der Benutzer dann dem Kontext beitritt, oder verweigert und somit der Antrag abgelehnt

Implementieren von Best Practices

Business Alignment

Zur erfolgreichen Durchführung eines Business Alignment müssen Vorgesetzte zusammen mit den Eigentümern von Anwendungen Rollen, Policies und Kontexte erstellen, die zur schnellen, präzisen Gewährung von Zugriffsrechten für Personen verwendet werden, die dem Unternehmen beitreten oder die Rolle wechseln.

PROZESS-STAKEHOLDERS

Business Alignment-Prozesse sind administrative Prozesse, die Endbenutzern und Vorgesetzten die Verwendung des IGA-Systems vereinfachen. Die Festlegung von Rollen, Policies und Kontexten übernehmen die Vorgesetzten in Absprache mit den Eigentümern von Anwendungen. Die Personalabteilung muss aber auch involviert werden, um sicherzustellen, dass Jobtitel unternehmensweit einheitlich verwendet werden, damit der Zugriff einheitlich gewährt wird.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
Personalabteilung (HR)	Die Personalabteilung sichert die Konsistenz von Jobtiteln im HR-System.	Die im HR-System gespeicherten Jobtitel müssen vereinheitlicht werden, damit Mitarbeitern, die die gleiche Tätigkeit ausüben, einheitliche Zugriffsrechte gewährt werden können.	Sicherstellen der Konsistenz der Jobtitel von Mitarbeitern mit den entsprechenden Positionen.	Vereinheitlichung von Jobtiteln, wenn neue Mitarbeiter dem Unternehmen beitreten, damit diesen die gleichen Zugriffsrechte gewährt werden können wie ihren Kollegen.
IGA-Team	Erstellen von Rollen, Policies und Kontexten, nachdem diese von den Vorgesetzten definiert wurden.	Das IGA-Team ist zuständig für die Erstellung von Rollen, Policies und Kontexten im IGA-System, nachdem diese zunächst für das Unternehmen definiert wurden.	Keine	Erstellung von Rollen, Policies und Kontexten je nach Definition und Anforderungen des Unternehmens.
Vorgesetzte	Unterstützung bei der Definition von verschiedenen Rollen innerhalb der einzelnen Teams sowie von Policies und Kontexten im übrigen Unternehmen.	Vorgesetzte haben Verantwortung für das Unternehmen und wissen daher, welche Informationen sie benötigen, um über Gewährung bzw. Ablehnung von Zugriffsrechten zu entscheiden.	Zusammenarbeit mit Personalabteilung, um sicherzustellen, dass Jobtitel positionsübergreifend einheitlich sind. Vorgesetzte sollten gemeinsam mit Führungskräften anderer Abteilungen für Einheitlichkeit im gesamten Unternehmen sorgen.	Kontinuierliche Definition von im Einklang mit geschäftlichen Anforderungen stehenden Rollen, Policies und Kontexten.
Endbenutzer	Endbenutzer sind nicht direkt an Prozessen des Business Alignment beteiligt. Sie profitieren aber letztlich davon, da das Alignment dem IGA-Team und den Vorgesetzten hilft, schneller und leichter Zugriff zu erhalten.	Keine	Keine	Keine

Wichtige Best Practices

Empfehlungen

Nachfolgend eine Reihe von Best-Practice-Empfehlungen, die bei der Umsetzung von Business Alignment-Prozessen in IdentityPROCESS+ bedacht werden sollten.

ROLLEN

Festlegen von Rollen-Governance-Prozessen
Zur erfolgreichen Verwendung rollenbasierter Modelle zur Vergabe von Zugriffsrechten für Personen bedarf es sorgfältig definierter Rollen. Dies stellt viele Organisationen vor Herausforderungen, da eine solche Aufgabe nicht immer von IGA-Projekten abgedeckt wird. Hat eine Organisation beschlossen, Zugriffsrechte rollenbasiert zu vergeben, ist das als Vorbild fungierende Modell aber nicht ausreichend entwickelt, verzögert sich das IGA-Projekt, bis das Modell fertig ist. Wichtig ist außerdem, dass das Rollenmodell nicht zu komplex ist, da dies die Definition der Regeln zur Funktionstrennung nur erschwert.

Sicherstellen, dass Endbenutzer Rollennamen verstehen können
Um die Gewährung von Zugriffsrechten zu beschleunigen, sind Rollen klar zu benennen, damit Mitarbeiter die richtige Rolle finden, die zu ihren Anforderungen passt, ohne auf das Helpdesk zurückzugreifen.

Erstellen von Rollen, die Compliance-Anforderungen unterstützen
Organisationen müssen sicherstellen, dass die Rollen, die sie innehaben, ohne allzu großen Aufwand leicht die in Compliance-Matrix einpassbar sind. Zu viele verschiedene Rollen sorgen nur für unnötige Komplexität, und das erschwert das Compliance Management.

EINSCHRÄNKUNGEN

Definieren von Einschränkungen auf Rollen- bzw. Businessprozess-Ebene
Einschränkungen zwischen einzelnen Rollen sollten auf Rollen- oder Geschäftsprozess-Ebene definiert werden, da Organisationen dadurch eine gute Übersicht und Verständnis für potenzielle Verstöße bewahren. Einschränkungen sollten eher in kaufmännischer als in technischer Fachsprache formuliert werden, damit die betreffenden Abteilungen wie z. B. die Finanz- oder Rechtsabteilung sicherstellen können, dass Anforderungen richtig definiert wurden.

KONTEXTE

Sicherstellen, dass mit Kontexten verbundene Zugriffsrechte entfernt werden, wenn ein Benutzer seine Mitwirkung beendet hat oder eine Terminierung erfolgt
Benutzern werden Zugriffsrechte gewährt, wenn diese einem Kontext zugewiesen werden. Es wird dringend empfohlen, diese Zugriffsrechte automatisch zu deaktivieren, wenn ein Benutzer einem bestimmten Kontext nicht mehr angehört. Wird beispielsweise ein Benutzer einem Kurzprojekt zugewiesen und ihm entsprechender Zugriff gewährt, sollten ihm die Zugriffsrechte automatisch verweigert werden, wenn er nicht mehr an dem Projekt beteiligt ist. Dies sichert Compliance und Sicherheit hinsichtlich des Zugriffs auf die Anwendungen des Projekts. Darüber hinaus sollten bei Entfernung eines Kontexts aus dem IGA-System auch alle den Benutzern aufgrund ihrer Zugehörigkeit zu einem Kontext gewährten Zugriffsrechte deaktiviert werden.

Zusammenfassung

Mit Business Alignment-Prozessen können Organisationen Benutzer leichter managen, weil sie diese dadurch in Gruppen zusammenführen können, die auf den von ihnen ausgeübten Tätigkeiten basieren (Rollen) oder auf den Gemeinsamkeiten in deren Jobs wie z. B. der Zugehörigkeit zur selben Projektgruppe oder dem Vorhandensein bestimmter Attribute, die sie verbinden wie z. B. die Zugehörigkeit zur selben Abteilung.

Die Fähigkeit zum Managen von Benutzern auf Basis bestimmter Kriterien verbessert nicht nur die Effizienz der IT-Abteilung – die Zugriffsrechte nicht mehr einzeln für Mitarbeiter vergeben muss –, sondern es verbessert auch die Aspekte Sicherheit und Compliance, da bestimmte Zugriffsrechte einmal zentral festgelegt und dann auf alle Benutzer mit identischen Anforderungen angewandt werden.

Prozessbereich

Management von Sicherheitsvorfällen

Hat eine Organisation den Verdacht, dass die Identität eines Benutzers gefährdet wurde, ist schnelles Handeln zur Begrenzung eventueller Schäden gefragt. Hat das Unternehmen seinen Prozess zum Reagieren auf Sicherheitsvorfälle noch nicht automatisiert, vergeudet die IT-Abteilung mit der Klärung der Frage, welchen Zugriff die Identität hat und mit deren individueller Sperrung in der Fachanwendung möglicherweise wertvolle Zeit.

Um dem entgegenzutreten, sollten folgende Managementprozesse bei Sicherheitsvorfällen integriert werden:

1. Administratoren haben die Möglichkeit, alle mit einer Identität verbundenen Konten zu deaktivieren.
2. Ein Administrator kann den Zugriff erneut aktivieren, nachdem die Situation wieder unter Kontrolle ist.

Der erste Schritt hindert Angreifer daran, weiterhin im Netzwerk zu agieren, vertrauliche oder sensible Daten zu stehlen oder betriebliche Abläufe durch Beschädigen von Daten bzw. Unbrauchbar-Machen wichtiger Anwendungen zu stören. Außerdem erhält ein Unternehmen durch das Sperren von Accounts, bei denen Verstöße festgestellt wurden, Zeit für fachliche Nachforschungen und zur Durchführung nicht-technischer Maßnahmen bei kritischen Sicherheitsvorfällen wie z. B. internes und externes Kommunikationsmanagement, Maßnahmen zum Schutz des guten Rufs von Unternehmen und Marke sowie zur Entgegennahme der Anrufe von Kundschaft und Presse.

Der zweite Schritt stellt sicher, dass nach Feststellung der Ursachen eines Verstoßes und im Anschluss an die von Sicherheitsexperten eingeleiteten Maßnahmen zur Vermeidung einer Wiederholung eines solchen Vorfalls die gesperrten Identitäten schnell reaktiviert werden und der Geschäftsbetrieb wieder aufgenommen werden kann.

Warum das Management von Sicherheitslücken wichtig ist:

1. Zur Begrenzung von Verlust bzw. Beschädigung sensibler Daten.
2. Zur Begrenzung der lateralen Bewegungsfähigkeit von Angreifern innerhalb des Netzwerks.
3. Zur Automatisierung von Notfallsperrungen infolge von Informations-Input durch andere Sicherheits-Monitoring-Tools.

Das IdentityPROCESS+ Framework erlaubt eine manuelle Initialisierung von Prozessen im Bereich Sicherheitsvorfälle. Darüber hinaus können Unternehmen hier auch anspruchsvollere Lösungen implementieren, indem sie die Notfallsperrung durch externe Sicherheitslösungen wie ein Security Information and Event Management (SIEM)-System, ein User and Entity Behavior Analytics (UEBA) System oder eine Threat Analytics-Lösung auslösen lassen. Da dieser Prozess automatisiert abläuft, erfolgt die Notfallsperrung noch schneller und schützt so die Infrastruktur der Organisation noch wirksamer.

Der Prozessbereich Sicherheitsvorfälle umfasst die folgenden Prozesse:

Zugriff dekativieren

- Notfallsperre
- Rücknahme der Notfallsperre

Prozess

Zugriff deaktivieren oder reaktivieren

Ermöglicht Administratoren die schnelle Deaktivierung von Benutzerkonten, bei denen Verdacht auf einen Verstoß besteht sowie die Reaktivierung der Konten nach Abschluss der Untersuchungen und Gegenmaßnahmen zur Vermeidung des neuerlichen Auftretens eines solchen Vorfalls.

NOTFALLSPERRE

Organisationen müssen die Benutzerkonten Einzelner schnell deaktivieren können, wenn der Verdacht besteht, dass ein oder mehrere Konten missbräuchlich verwendet wurden, um die Angreifer daran zu hindern, die Netzwerkerkundung fortzusetzen, vertrauliche oder sensible Daten zu stehlen oder betriebliche Abläufe durch Beschädigen von Daten bzw. Unbrauchbar-Machen wichtiger Anwendungen zu stören.

Prozessbeschreibung

Wurde ein Benutzerkonto angegriffen, greift die Notfallsperrung: Sie setzt die Identität auf „gesperrt“ und deaktiviert für die betreffende Identität den Zugriff zu allen Systemen. Um die Sperrung möglich zeitsparend durchzuführen, überspringt der Prozess die Einholung einer Genehmigung beim Vorgesetzten des betreffenden Mitarbeiters – was in so einem Fall das normale Vorgehen wäre. Daher sollte ein solches Vorgehen nur in Notfällen oder auf behördliches Ersuchen angewandt und ein entsprechender Prozess in den Unternehmensrichtlinien niedergelegt werden.

Best-Practice-IGA-System-Funktionalität

Ein Manager oder operativer Administrator leitet die Notfallsperrung im IGA-System ein und wählt die zu sperrende Identität aus. Für Auditzwecke muss ein Grund eingegeben werden, warum die Identität gesperrt wird. Das IGA-System setzt die Identität auf „locked“ und den Zuweisungsparameter auf „disabled“. Wird eine Identität auf „locked“ gesetzt, kann dieser Status nicht durch eine externe Schnittstelle geändert werden.

Technischer Prozessablauf

1. Verdacht auf einen Sicherheitsverstoß bedeutet, dass Sofortmaßnahmen nötig sind.
2. Ein Manager oder operativer Administrator leitet den Notfallsperrprozess ein.
3. Manager können beliebige von ihnen gemanagte Identitäten blockieren und müssen für Audit-Zwecke eine Begründung hierfür angeben.
4. Operative Administratoren können beliebige Identitäten blockieren und müssen für Audit-Zwecke eine Begründung hierfür angeben.
5. Die gewählte Identität wird auf „locked“ und der Vorgang auf „disabled“ gesetzt.

NOTFALLSPERRE AUFHEBEN

Ist die Notfallsperrung für eine Identität nicht mehr erforderlich, müssen Manager und operative Administratoren diese rasch entsperren, damit die Benutzer wieder Zugriff auf ihre Systeme erhalten und weiterarbeiten können.

Prozessbeschreibung

Nach erfolgreicher Lösung einer Kontensperrung in der Organisation können Manager und operative Administratoren die gesperrten Identitäten wieder aktivieren. Dadurch wird erneut der Zugriff auf alle Zielsysteme der Identität möglich.

Best-Practice-IGA-System-Funktionalität

Ein Manager oder operativer Administrator leitet die Aufhebung der Notfallsperrung im IGA-System durch Auswahl der zu entsperrenden Identität ein. Für Auditzwecke muss ein Grund eingegeben werden, warum die Identität wieder entsperrt wird. Das IGA-System setzt dann die Identität auf „unlocked". Der Zuweisungsparameter wird wieder auf „active" gesetzt.

Technischer Prozessablauf

1. Der Verdacht auf einen einen Verstoß erweist sich entweder als substanzlos oder die Sicherheitslage wird bereinigt.
2. Ein Manager entsperrt entweder alle von ihm verwalteten Identitäten oder ein operativer Administrator entsperrt einzelne gesperrte Identitäten.
3. Für Auditzwecke wird ein Grund für die Entsperrung angegeben.
4. Die Identität wird auf „unlocked" und die Zuweisungen auf „disabled" gesetzt.

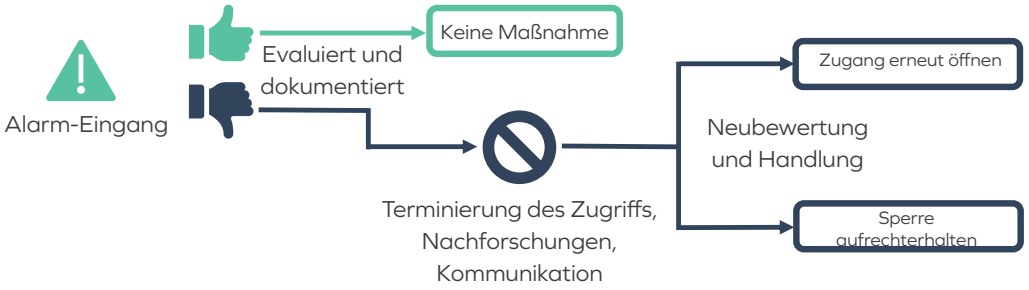


Abb. 4: Management von Sicherheitsvorfällen (vereinfachte Darstellung)

! QUICK WIN...

Good Governance:
Bereitschaft zur Durchsetzung von Policies im Bereich Sicherheitslücken sowie, bei Verdacht auf einen Verstoß, zur sofortigen Einleitung einer Notfallsperrung

Sicherheitsvorfälle

PROZESS-STAKEHOLDER

Eingeleitet werden Prozesse im Bereich Sicherheitsvorfälle vom IGA-Team, da dieses darauf geschult ist, die Implikationen von Notfallsperrungs-Verfahren zu verstehen. Aufgrund der Beschaffenheit potenzieller Vorfälle, die diese Prozesse auslösen könnten (z. B. Missbrauch von Computer-Ressourcen durch Mitarbeiter), muss die Personalabteilung sicherstellen, dass Policies vorhanden sind, die bei jedem potenziellen Verstoß umgesetzt werden.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
Personalabteilung (HR)	Es ist sicherzustellen, dass HR-Richtlinien eingehalten werden.	Da im Zuge der Prozesse im Bereich Sicherheitsvorfälle auch Benutzer wegen Missbrauchs von Unternehmensressourcen gesperrt werden könnten, muss die Personalabteilung sicherstellen, dass sämtliche Policies umgesetzt werden.	Sicherstellen, dass Policies zur Steuerung von Prozessen im Bereich Sicherheitsvorfälle schriftlich niedergelegt sind	Bereitschaft zur Durchsetzung von Policies im Bereich Sicherheitsvorfälle.
IGA-Team	Das IGA-Team leitet den Prozess der Notfallsperrung bei Verdacht auf einen Sicherheitsverstoß oder internen Missbrauch ein.	Das IGA-Team wird darauf geschult, die Implikationen des Notfallsperrungs-Verfahrens zu verstehen. Hier besteht auch Einigkeit darüber, was zur Vermeidung weiterer Verstöße oder für Follow-up-Gespräche mit Mitarbeitern vor Wiederherstellung des Zugriffs zu tun ist.	Durchführung von Schulungen zu den Folgen der Einleitung von Notfallsperrungen und zur Wiederherstellung von Benutzerzugängen.	Bereitschaft zur Einleitung einer Notfallsperrung bei Verdacht auf einen Verstoß.

Wichtige Best Practices

Empfehlungen

Nachfolgend eine Reihe von Best-Practice-Empfehlungen, die bei der Umsetzung von Prozessen hinsichtlich Sicherheitsvorfällen bei IdentityPROCESS+ bedacht werden sollten.

Schriftliches Niederlegen eines bei Sicherheitsverstößen anzuwendenden Prozesses

Die Anwendung des Prozesses bei Sicherheitsverstößen ist sorgfältig abzuwägen, da hierbei Personen am Zugriff auf Systeme gehindert werden. Zu den möglichen Negativfolgen der Anwendung dieses Prozesses zählen die unnötige Beschränkung des Zugriffs eines Benutzers auf wichtige Geschäftssysteme bzw. -ressourcen aufgrund des Verdachts auf externe oder interne Sicherheitsverstöße – wodurch Kollegen an der Durchführung ihrer Aufgaben gehindert werden.

Da es aber auch Situationen gibt, in denen die Sperrung des Zugriffs eines Benutzers völlig legitim ist – z. B. wenn ein Sicherheitsverstoß entdeckt wird oder die missbräuchliche Verwendung von Systemen offensichtlich ist – wird dieser Prozess gelegentlich Anwendung finden. Daher ist es wichtig, dass die Organisation über eine formale Policy verfügt, die regelt, wie dieser Prozess anzuwenden und was hierbei zu beachten ist.

Sicherstellen einer selektiven Anwendung der Notfallsperrung

Da die Gründe für eine Notfallsperrung heikel sein können – z. B. Sicherheitsverstöße oder ein unaufrichtiger Mitarbeiter – sollten Organisationen Maßnahmen einführen, um die Zahl der Mitarbeiter zu begrenzen, die Kenntnis von dem Vorfall haben. Erweist sich der Verdacht nämlich als unbegründet, beschränkt dies sowohl interne Spekulationen als auch Verstöße gegen persönliche Vertraulichkeitsauflagen. Zeigt sich, dass die Notfallsperrung gerechtfertigt ist, erfolgen sowohl erforderliche Maßnahmen wie z. B. interne Disziplinarverfahren als auch strafrechtliche Ermittlungen unbeeinflusst von Spekulationen.

?

Fragen, die man sich im Themenbereich Sicherheitsvorfälle stellen sollte

- Ist das Vorgehen bei Verdacht auf Sicherheitsverstöße schriftlich niedergelegt?
- Welche Stakeholder sollten involviert werden?
- Gibt es einen Prozess, der den Kreis derjenigen einschränkt, die wissen, wie Prozesse rund um Sicherheitsverstöße eingeleitet werden?
- Wie geht man zur Rückgängigmachung einer irrtümlich eingeleiteten Notfallsperrung vor?

ZUSAMMENFASSUNG

Prozesse im Bereich Sicherheitsvorfälle erleichtern Administratoren das vorübergehende Sperren des Benutzerzugriffs, wenn der Verdacht besteht, dass Konten entweder durch die Benutzer oder externe Angreifer für missbräuchliche Zwecke verwendet werden. Aufgrund der hohen Wirksamkeit dieses Prozesses ist er sorgfältig anzuwenden und zu dokumentieren. Außerdem muss jede Person, die ihn anwendet, seine Implikationen verstehen.

Prozessbereich

Governance

Heutzutage genügt es nicht, mehr, dass Organisationen externe Bestimmungen und interne Policies einhalten. Das Bekanntwerden von Fällen, in denen Unternehmen Angriffe oder Datenverstöße einräumen mussten, zeigen, dass der Nachweis von Compliance ein essenzielles Element jeder unternehmerischen Tätigkeit ist.

Für viele Unternehmen ist es eine komplexe Aufgabe, zu dokumentieren, wer warum auf welche Ressourcen zugreifen kann. Mögliche Vorgehensweise: Die Manager bitten, den Zugriff durch ihre direkt unterstellten Mitarbeiter zu prüfen. Dieser Ansatz ist zwar sinnvoll, kann aber dazu führen, dass Vorgesetzte Zugriffsberechtigungen einfach nur „durchwinken", weil die abzuarbeitende Liste sehr lang werden kann. Und vielleicht sind sie auch nicht genug am Puls der täglichen Aufgaben, um genau zu wissen, welche Art von Zugriff ihre Mitarbeiter zur Wahrnehmung ihrer täglichen Aufgaben brauchen.

Schaffung von Transparenz beim Thema Zugriff
Durch die Prozesse im Bereich Governance können Organisationen prüfen, wer auf welche Informationen zugreift, nicht mehr erforderliche Zugriffsrechte deaktivieren, Echtzeit- und historische Auditberichte erstellen, um Zugänge transparent zu machen und die ordnungsgemäße Umsetzung von Policies zur Funktionstrennung (SoD) sicherzustellen.

Dieser Prozessbereich besteht aus mehreren Prozessen, die verschiedene Governance-Aspekte anvisieren.

Warum Governance Management wichtig ist:

1. Stellt sicher, dass Benutzer nur die Zugangsrechte erhalten, die sie brauchen, um ihre Aufgaben wahrzunehmen.
2. Ermöglicht Eigentümern von Anwendungen und Vorgesetzten die Möglichkeit zur Sicherstellung des passenden Zugriffs-Levels.
3. Durchsetzung von Policies zu Datenschutzbestimmungen und Konflikten bei Zugangsrechten.

Governance

Sicherstellung von Konten-Sicherheit und -Compliance
Die Benutzern beim Eintritt in ein Unternehmen oder bei der Beantragung neuer Zugriffsrechte gewährten Rechte sind möglicherweise nicht während des gesamten Lebenszyklus der Identität erforderlich. Werden Zugriffsrechte nicht in regelmäßigen Abständen überprüft, häufen die Benutzer in der Regel Rechte an, die über ihre tatsächlichen Anforderungen hinausgehen. Durch Governance-Prozesse können Administratoren mit den Eigentümern von Anwendungen oder Vorgesetzten von Mitarbeitern sicherstellen, dass der Zugriff, der Benutzern gewährt wurde, im Einklang mit ihrer gegenwärtigen Tätigkeit steht.

Wird ein Konto entdeckt, dem kein Eigentümer zugeordnet ist (ein so genanntes „verwaistes Konto"), weil der Mitarbeiter das Unternehmen verlassen hat, ermöglichen Governance-Prozesse je nach Fall entweder die Neuzuweisung oder die Terminierung des Kontos.

Überwacht werden muss aber nicht nur der Zugriff auf Systeme, sondern auch, welche Datentypen abgerufen werden. Durch Governance-Prozesse können Administratoren, Dateneigentümer und Manager, den in ihren Systemen gespeicherten Informationen, verschiedene Risikoklassifikationen zugeordnet werden. Sind diese Klassifikationen einmal zugeordnet, kann der Datenzugriff im Einvernehmen mit verschiedenen globalen Datenschutzbestimmungen und anderen geltenden Datenschutzstandards gesteuert werden.

Wahrung kontinuierlicher Compliance
Die Prüfung der Frage, ob der Ist-Zustand des Benutzer gewährten Zugriffs mit dem Soll-Zustand – der ein regelkonformes und sicheres System gewährleistet – übereinstimmt, ist ein zentraler Prozess guter Governance. Hierbei entdeckte Unstimmigkeiten werden dem Administrator gemeldet und der Zugriff dementsprechend gewährt oder verweigert.

Darüber hinaus umfassen Governance-Prozesse auch Workflows zum Managen der Regel zur Funktionstrennung (SoD). Dies verhindert die Gewährung riskanter Zugriffskombinationen an einzelne Personen und somit auch die Durchführung betrügerischer Handlungen.

Der Prozessbereich Governance umfasst die folgenden Prozesse:

Bericht generieren
- Reporting

Rezertifizierung durchführen
- Rezertifizierungskampagne erstellen
- Rezertifizierungskampagnen verwalten
- Fragen rund um die Kampagne beantworten
- Ownership übertragen
- Details des Kontenbesitzes für ein System anzeigen
- Starten einer Berechtigungs-Rezertifizierung für Manager / Rechte-Eigentümer

Abgleich durchführen
- Soll-/Ist-Abgleich durchführen

Datenklassifizierung vornehmen
- Klassifizierungs-Tags zuweisen
- Datenobjekte mit Klassifizierungs-Tags versehen

Funktionstrennung (SoD)
- Verstoß bewerten

Prozess

Bericht generieren

Schafft Transparenz bei Zugriffsrechten für alle Anwendungen in der Organisation und somit kontinuierliche Sicherheit und Compliance.

REPORTING

Transparenz bei Zugriffsrechten in allen Anwendungen in der gesamten Organisation ist ein Schlüsselelement von Sicherheit und Compliance. Durch Echtzeit-Dashboards können Organisationen ihre aktuelle Zugriffssituation unter Compliance-Aspekten bewerten und gegen evtl. Verstöße entsprechend vorgehen. Anhand von Verlaufsberichten können sie ihre Compliance für Auditzwecke nachweisen.

Prozessbeschreibung

Im Zuge des Reporting-Prozesses werden Verlaufsdaten aus dem Datenspeicher extrahiert, die Angaben zu relevanten Objekten machen. Die Berichte liefern umfassende Datenübersichten, die Fragen beantworten wie z. B. wer warum auf was Zugriff hat, wann die Genehmigung durch wen erteilt bzw. entzogen wurde. Auch Verstöße gegen Regelungen zur Funktionstrennung (SoD) werden gemeldet. Audittaugliche Berichte mit Angaben über die Protokollierung und Genehmigungen ermöglichen den On-Demand-Zugriff auf Berichte und Dokumentation für Auditoren.

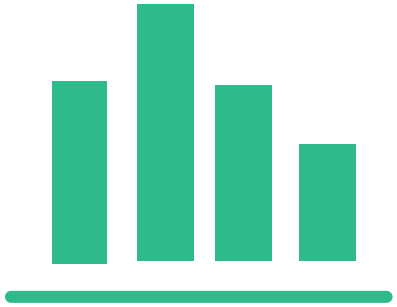
Best-Practice-IGA-System-Funktionalität

Aus dem Datenspeicher des IGA-Systems extrahierte Daten werden, je nach geschäftlicher Anforderung, zur Erstellung verschiedener Berichte herangezogen. Auf konfigurierbaren Dashboards werden Live-Daten mit KPIs (Vergleich von Ist-Zahlen mit Schwellenwerten) und andere Echtzeit-Charts angezeigt. Listenansichten enthalten aktuelle Listen mit Datenobjekten, und Data-Warehouse-Reports generieren zu Auditzwecken Verlaufsdaten, die zeigen, wer wann auf was Zugriff hatte.

Zu Reporting Zwecken können Listenansichten als CSV- oder PDF-Datei heruntergeladen werden.

Technischer Prozessablauf

1. Ein Benutzer ruft mit dem Browser den gewünschten Bericht auf und gibt alle optionalen Parameter wie Zeit, Identität, System und Ressource ein
2. Das System überprüft, ob der Benutzer berechtigt ist, Daten aus der Datenbank auszulesen und präsentiert die Daten im Bericht
3. Der Benutzer speichert den Bericht als Excel-, CSV- oder PDF-Datei und kann ihn so mit anderen teilen



Prozess

Rezertifizierung durchführen

Unternehmen können konstante Compliance sichern, indem sie Manager und Ressourcen-Eigentümer anhalten, zu prüfen, ob die tatsächlichen Zugriffsrechte, die Benutzer von Anwendungen besitzen, noch gültig sind bzw. ggf. erforderliche Anpassungen vorzunehmen.

REZERTIFIZIERUNGSKAMPAGNE ERSTELLEN

Zur Sicherung kontinuierlicher Sicherheit und Compliance muss regelmäßig überprüft werden, dass Informationen wie z. B. in IGA-Systemen gespeicherte Zugriffsrechte, Policies, Rollendefinitionen und Stammdaten noch aktuell sind.

Um erfolgreich zu sein, müssen die angewandten Prozesse so einfach und effizient wie möglich zu erstellen sein, damit sie von denen, die sie umsetzen sollen, nicht als zusätzliche Belastung empfunden werden.

Prozessbeschreibung

Rezertifizierungs-Kampagnen – auch als Reviews, Attestierungen oder Rezertifizierungen bezeichnet – werden zur periodischen Validierung von im IGA-System gespeicherten Informationen herangezogen. Der Design-Prozess für Rezertifizierungskampagnen gestattet Administratoren auch die Gestaltung ganz individueller Kampagnen.

Abläufe im IGA-System

Der Administrator definiert den Zweck der Kampagne einschließlich der zu zertifizierenden Daten, der hierfür zuständigen Person(en) und der Häufigkeit, mit der die Umfrage im IGA-System durchzuführen ist. Der Administrator macht darüber hinaus Angaben, was passieren sollte, wenn Antworten eintreffen bzw. ausbleiben, welche Benachrichtigungen und Erinnerungen versandt werden sollten. Außerdem legt er fest, wer die Kampagne überwacht und managt. Nachdem der Administrator die Kampagne aufgesetzt hat, können im IGA-System ein Test sowie danach ggf. Anpassungen durchgeführt werden.

Technischer Prozessablauf

1. Festlegung der Parameter für die Rezertifizierungskampagne.
2. Erstellung der Rezertifizierungskampagne.
3. Test sowie ggf. Anpassung der Rezertifizierungskampagne.

VERWALTEN VON REZERTIFIZIERUNGSKAMPAGNEN

Das Managen von Rezertifizierungskampagnen umfasst auch deren Start sowie die Durchführung allgemeiner Verwaltungsaufgaben und deren Abschluss.

Prozessbeschreibung

Ein Rezertifizierungs-Administrator initiiert Umfragen und weist sie den zuständigen Managern bzw. System-Eigentümern zu. Zur Administration zählt die Entscheidung, wann die Kampagne beginnt, sowie Fortschritts-Monitoring, ggf. Stellen anderer Fragen auf Bitten der befragten Person, das Erstellen und Versenden von Berichten an Stakeholder sowie der Abschluss der Rezertifizierung.

Best-Practice-IGA-System-Funktionalität

Das IGA-System gibt Administratoren eine Schnittstelle an die Hand, mit der sie die im Rezertifizierungskampagnen-Prozess erstellte Umfrage starten können. Sie können damit auch Informationen hinzufügen, den Antwort-Status von Umfragen abrufen, die Umfrage schon vor Beantwortung aller Fragen beenden, falls keine Relevanz mehr besteht und außerdem Berichte erstellen.

Technischer Prozessablauf

1. Eine im Rezertifizierungskampagnen-Prozess erstellte Umfrage basiert auf Faktoren wie Risikoklassifikation, Systeme und Ressourcentypen
2. Die Umfrage wird erstellt und geprüft
3. Start der Umfrage
4. Der Administrator kann die Umfrage auch schließen, wenn er der Meinung ist, dass die darin gestellten Fragen nicht mehr relevant sind
5. Hat die befragte Person alle Fragen beantwortet, schließt die Umfrage und wird auf „abgeschlossen“ gesetzt. Abschließend werden vom Administrator festgelegte System-Maßnahmen durchgeführt.
6. Der Administrator generiert einen PDF-Bericht

! QUICK WIN...

Nachweis der Compliance für Auditoren: Erstellen von Berichten in Echtzeit, zu bestimmten Zeitpunkten oder Generieren von Verlaufsprotokollen

BEANTWORTUNG VON FRAGEN RUND UM DIE KAMPAGNE

Im IGA-System gespeicherte Informationen müssen von Vorgesetzten oder System-Eigentümern aktualisiert und validiert werden, um sicherzustellen, dass Entscheidungen auf Basis möglichst aktueller und präziser Informationen getroffen werden.

Prozessbeschreibung

Nachdem der Administrator die Kampagne eingeleitet hat, werden alle Fragen an einzelne Personen weitergeleitet, damit Antworten gegeben werden können. Fragen, die nicht automatisch zugewiesen werden können, werden vom Administrator der Umfrage manuell verteilt. An die befragte Person wird die Aufgabe verschickt, die Fragen der Kampagne zu beantworten.

Best-Practice-IGA-System-Funktionalität

Wurde die Kampagne vom Administrator gestartet, wird dem Manager eine Prüfungsaufgabe zugewiesen. Das System fordert nicht, dass der Manager alle Fragen auf einmal beantwortet und zeigt über eine Fortschrittsanzeige an, wie viel noch unbearbeitet ist.

Technischer Prozessablauf

1. Der Reviewer wird mit der Aufgabe betraut, Daten (wie z. B. Zugriffsrechte für gemanagte Identitäten) zu rezertifizieren.
2. Der Reviewer prüft die Daten.
3. Der Reviewer beantwortet die Fragen, fügt bei Bedarf auch Kommentare hinzu.
4. Kann der Reviewer die eine oder andere Frage nicht beantworten, können diese – das Einverständnis des Administrators vorausgesetzt – auch an andere weitergeleitet werden. Hat der Administrator der Umfrage die Neuzuweisung von Fragen nicht gestattet, kann der Reviewer den Administrator bitten, Fragen neu zuzuweisen.

ÜBERTRAGUNG VON OWNERSHIP

Zur Sicherung kontinuierlicher Sicherheit und Compliance müssen Objekte, denen bei Terminierung einer Identität kein Eigentümer zugewiesen ist, einer anderen Identität zugewiesen werden.

Prozessbeschreibung

Verlässt ein Mitarbeiter oder Externer das Unternehmen und wird seine Identität deaktiviert, muss das Unternehmen die Eigentümerschaft für Objekte auf eine andere menschliche Identität übertragen.

Dieser Prozess löst automatisch einen Workflow aus, der es Ressourcen-Eigentümern ermöglicht, neue Eigentümer vorzuschlagen, die den Vorschlag dann annehmen oder ablehnen können.

Best-Practice-IGA-System-Funktionalität

Die Transfer-Ownership-Umfrage beginnt unmittelbar nach Terminierung der Identität und die zuzuweisenden Personen werden nach Objekttyp ausgewählt. Die Umfrage managt die Eigentümerschaft technischer und humaner Identitäten, Organisationseinheiten, Ressourcen, Ressourcen-Ordnern und Systemen. Wird ein neuer Objekteigentümer vorgeschlagen und der Vorschlag angenommen, nimmt das IGA-System die entsprechende Änderung vor.

Technischer Ablauf

1. Terminierung der Identität.
2. Es wird eine Umfrage zum Transfer-Ownership von Objekten eingeleitet.
3. Neue Eigentümer werden vorgeschlagen.
4. Der neue Eigentümer des jeweiligen Projekts akzeptiert den Vorschlag.
5. Die Eigentümerschaft des Objekts hat sich geändert.

KONTENEIGENTÜMER

Zur Gewährleistung von Compliance muss jedem Konto ein Eigentümer zugewiesen sein. Können die Regeln im IGA-System den Eigentümer eines verwaisten Kontos nicht ermitteln, muss manuell ein neuer Eigentümer zugewiesen werden.

Prozessbeschreibung

Ist die Daten-Qualität im IGA-System nicht ausreichend und decken die definierten Account-Ownership-Regeln nicht alle Konten im Zielsystem ab, muss der Eigentümer des verwaisten Kontos manuell zugewiesen werden. Beim Account-Ownership-Prozess können sowohl neue Eigentümer verwaister Konten manuell vorgeschlagen als auch Deprovisionierungsmaßnahmen eingeleitet werden, wenn das entsprechende Konto nicht mehr benötigt wird, weil der Eigentümer das Unternehmen verlassen hat. Nach Abschluss des Prozesses wurden den verwaisten Konten entweder neue Eigentümer zugewiesen, oder die Konten wurden deaktiviert.

Best-Practice-IGA-System-Funktionalität

Das IGA-System zeigt die verwaisten Konten an und ermöglicht dem System-Eigentümer so den Start des Account-Ownership-Prozesses. Der System Eigentümer schlägt für jedes verwaiste Konto neue Eigentümer vor.

Dem vorgeschlagenen Eigentümer wird eine Frage in Form einer Aufgabe zugesandt; er erhält dadurch Gelegenheit, die Eigentümerschaft anzunehmen oder abzulehnen. Der „manuelle Match" wird in der Stammdatenbank festgehalten und vermerkt, dass die Zuweisung nicht anhand von Regeln im IGA-System erfolgte.

Technischer Prozessablauf

1. Der System-Eigentümer leitet den Account-Ownership-Prozess ein und prüft die verwaisten Zuweisungen.
2. Der System-Eigentümer leitet eine Account-Ownership-Prüfung ein.
3. Der System-Eigentümer schlägt für die verwaisten Konten neue Eigentümer vor
4. Der vorgeschlagene Konteneigentümer nimmt die Eigentümerschaft für das vor kurzem verwaiste Konto an oder lehnt sie ab.

BERECHTIGUNGS-ZUWEISUNGSPRÜFUNG FÜR MANAGER/RECHTE-EIGENTÜMER

Die regelmäßige Überprüfung aller Zugriffsrechte von gemanagten Identitäten ist sinnvoll. Stellt ein Manager bei dieser Prüfung fest, dass Zugriffsrechte nicht angemessen sind, sollten sie dem Benutzer entzogen werden, um ein hohes Maß an Sicherheit und Governance zu gewährleisten.

Prozessbeschreibung

Zugriffsprüfungen werden entweder anhand von festen Zeitplänen oder manuell von System-Eigentümern, Daten- oder Systemadministratoren initiiert. Sie können Konten nach System, Organisationseinheit, speziellen Ressourcen, Compliance-Status oder Klassifizierungsmerkmalen prüfen. Trifft die Rezertifizierungsumfrage beim Manager oder Ressourcen-Eigentümer ein, entscheiden sie, ob der Benutzer Zugriff der betreffenden Identitäten aufrechterhalten oder entzogen wird.

Best-Practice-IGA-System-Funktionalität

Das IGA-System versendet eine Anfrage bzgl. einer Umfrage, die entweder auf Basis eines Zeitplans oder durch einen System-Eigentümer, Daten- oder Systemadministrator an den prüfenden Manager geleitet wird. Der prüfende Manager kann entscheiden, ob er den Zugriff zu den Identitäten behält oder entfernt. Direkte Zuweisungen ohne SOLL-Zustand in OIS werden sofort deaktiviert und deprovisioniert. Verfügt eine Zuweisung, die beibehalten wurde, bereits über den Soll-Zustand, bleibt diese unverändert und Zuweisungen mit vorherigem Soll-Zustand erhalten dann das Prädikat „Soll-Zustand".

Technischer Prozessablauf

1. Der Start einer Umfrage erfolgt entweder auf Basis eines Zeitplans oder durch einen System-Eigentümer, Daten- oder Systemadministrator.
2. Der prüfende Manager beantwortet die Fragen der Umfrage.
3. Direkte Zuweisungen ohne SOLL-Zustand in OIS werden deprovisioniert.
4. Hält ein Manager oder Ressourcen-Eigentümer eine existierende Zuweisung, der noch kein Soll-Zustand zugewiesen wurde, aufrecht, wird dieser als Soll-Zustand zugewiesen.
5. Alle abgelaufen Zuweisungen werden deaktiviert.

Prozess

Abgleich durchführen

Zeigt alle Diskrepanzen zwischen den von der Organisation angestrebten Sicherheits- und Compliance-Anforderungen auf, damit Administratoren entsprechende Korrekturmaßnahmen einleiten können.

SOLL-/IST-ABGLEICH DURCHFÜHREN

Zur Sicherstellung der von der Organisation angestrebten Sicherheits- und Compliance-Levels muss das IGA-System prüfen, ob der erwünschte Sicherheits- und Compliance-Status mit dem den System-Ressourcen gewährten tatsächlichen Zugriffsrechten übereinstimmt. Liegt eine Fehlzuweisung vor, müssen die Abweichungen zur Wahrung von Sicherheit und Compliance korrigiert werden.

Prozessbeschreibung

Der Abstimmungsprozess vergleicht den Ist-Zustand der Zielsysteme – die aktuellen Zugriffsrechte für jede Fachanwendung – mit dem Soll-Zustand, also der Idealbeschreibung für Sicherheit und Compliance in der Organisation. Die Unterschiede werden dem Administrator gemeldet, damit sie geprüft und Gegenmaßnahmen ergriffen werden können.

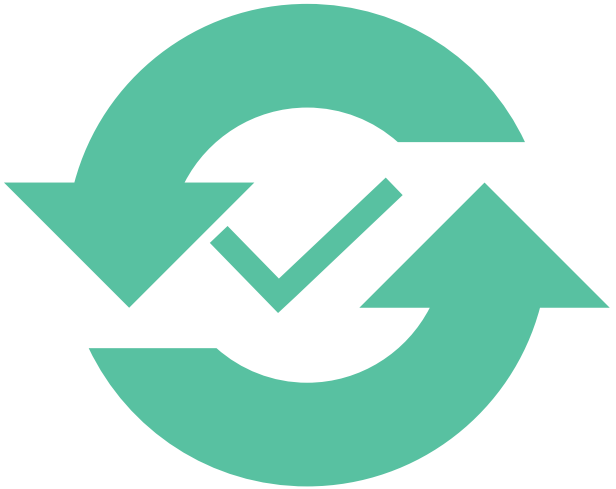
Best-Practice-IGA-System-Funktionalität

Das IGA-System vergleicht den vorgegeben Soll-Zustand mit dem in den Zielsystemen ermittelten Ist-Zustand und stellt den Compliance-Status grafisch dar.

Der Compliance-Status zeigt an, ob eine Zuweisung „unter Kontrolle" ist, d.h. ob sie explizit oder implizit genehmigt wurde. Andere Möglichkeiten beim Compliance-Status sind: nicht genehmigt, verwaiste Zuweisung, ausstehende Deprovisionierung, Verstoß, oder implizit zugewiesen.

Technischer Prozessablauf

1. Der „Soll-Zustand" wird im IGA-System definiert.
2. Das IGA-System stellt die Zugriffsrechte (den „Ist-Zustand") von den Zielanwendungen zusammen.
3. Das IGA-System nimmt einen Abgleich per Soll-/Ist- Vergleich vor, indem den Rechtezuweisungen ein Status zugewiesen wird.
4. Alle möglichen Diskrepanzen in Form der vergebenen Statuswerte zwischen Soll- und Ist-Zustand werden vom IGA-System grafisch angezeigt, damit der Administrator evtl. Abweichungen korrigieren kann.



Prozess

Systeme und Data-Store-Klassifizierung

Ermöglicht die Klassifizierung von Ressourcen auf Basis der gespeicherten Daten, wodurch Organisationen diverse Policies anwenden können, um verschiedene Compliance-Levels auf Basis interner und externer Bestimmungen zu realisieren.

ZUWEISUNG VON KLASSIFIZIERUNGS-TAG

In Abhängigkeit von Faktoren wie z. B. gespeicherten Daten, Sensibilität der gespeicherten Daten sowie allen deren Verwendung steuernde Bestimmungen müssen Ressourcen unterschiedlich gemanagt werden. Die Anwendung von Klassifizierungskennzeichen auf Identitäten, Systeme, Ressourcen, Ressourcen-Ordner, Kontexte und andere Objekte bringt eine leichte Erkennbarkeit mit sich, wenn spezielle Unternehmensprozesse Anwendung finden.

Prozessbeschreibung

Klassifikationskennzeichen und deren Kategorien (Gruppen solcher Kennzeichen) werden Objekttypen hinzugefügt, damit Organisationen Unternehmenspolicies und rechtlich vorgeschriebene Bestimmungen einhalten können. Kennzeichen ermöglichen Organisationen die Umsetzung ihrer Risiko-Management-Strategie und die Anwendung entsprechender Kontrollmechanismen. Über vordefinierte Klassifikationskennzeichen hinaus können und sollten noch weitere Klassifikationskennzeichen und -kategorien passend zum Unternehmensprofil und dem nationalen Kontext, in dem die Organisation operiert, definiert werden.

Best-Practice-IGA-System-Funktionalität

Daten-Administratoren schaffen im IGA-System eine aus einer Gruppe von Kennzeichen bestehende Kategorie von Klassifikationskennzeichen. So sollte z. B. die Klassifizierungskategorie „DSGVO“ mit Angaben zu „persönlichen Daten“, „sensiblen persönlichen Daten“, „hochriskanten Daten“, „mittelriskanten Daten“ sowie „kaum riskanten Daten“ befüllt werden.Anhand dieser Klassifikationen kann ein Administrator verschiedene Datentypen nach deren Sicherheits- und Compliance-Anforderungen managen.

Technischer Prozessablauf

1. Die geltenden Gesetze und Bestimmungen werden geprüft, um festzustellen, welche Daten zu klassifizieren sind.
2. Data-Mining benennt die erforderlichen Klassifizierungskategorien und -merkmale.
3. Die Klassifizierungskategorien werden nach Zielen validiert.
4. Es erfolgt eine Risikobewertung der neuen Klassifizierung mit Blick auf Gesetze und Bestimmungen.
5. Es werden Klassifizierungseigentümer ausgewählt, die die Klassifizierung von Objekten genehmigen können.
6. Die neuen Klassifizierungen werden nach Unternehmenszielen und -zwecken beschrieben.
7. Es werden Klassifizierungskampagnen für zu klassifizierende Objekte eingeleitet.

DATENOBJEKTE MIT KLASSIFIZIERUNGSTAGS VERSEHEN

Dateneigentümer müssen die in verschiedenen Ressourcen gespeicherten Daten identifizieren, damit diese den geeigneten Sicherheits-Levels und Compliance-Policies der Organisation zugewiesen werden können. Nach erfolgter Klassifizierung können die Daten identifiziert und entsprechend gemanagt werden.

Prozessbeschreibung

Wurden Klassifikationskennzeichen mit entsprechenden Kategorien eingerichtet, erfolgt die Kennzeichnung von Datenobjekten beispielsweise Verwendung einer Kampagne. Diese Klassifikationskennzeichen und ihre Kategorien dienen der Festlegung einer Risiko-Management-Strategie und führen durch Anwendung bestimmter Regeln relevante Risikoprüfungen ein.

Best-Practice-IGA-System-Funktionalität

Der Sicherheitsbeauftragte kann im IGA-System eine Umfrage erstellen, die dann an Benutzer versandt wird. Der Benutzer wird darin gebeten, die Informationen zu klassifizieren. Nach Beantwortung der Umfrage leitet das IGA-System die Klassifizierungen zur Genehmigung weiter. Nach Genehmigung werden Klassifikationskennzeichen dem Objekt hinzugefügt oder entzogen.

Technischer Prozessablauf

1. Gestartet wird die Umfrage von einem Systemadministrator oder Sicherheitsbeauftragten.
2. Die Fragen der Umfrage werden niedergeschrieben und vorab durchgesehen.
3. Die Umfrage beginnt.
4. Benutzer werden um Klassifizierung von Daten gebeten.
5. Der Benutzer beantwortet die Klassifizierungsumfrage.
6. Der Benutzer kann auch beantragen, dass die Frage wieder an den Administrator zurückgeht, wenn er meint, dass er zur Beantwortung nicht die geeignete Person ist.
7. Die übermittelte Klassifizierung geht dann an die zuständige Person, die die Klassifizierung genehmigt oder ablehnt.

! QUICK WIN...

Unterstützung der Risikomanagement-Strategie durch sinnvolle Nutzung von Klassifikationskennzeichen und -kampagnen zur Identifizierung kritischer und sensibler Daten

Prozess

Funktionstrennung (SoD)

Automatische Erkennung der Genehmigung aller riskanten Zugriffskombinationen, wodurch Endbenutzer daran gehindert werden sollen, unberechtigt auf Anwendungen zuzugreifen und dabei evtl. betrügerische Handlungen vorzunehmen.

BEWERTUNG VON VERSTÖSSEN

Die automatische Bewertung von Segregation-of-Duties-Policies muss durchgeführt werden, um sicherzustellen, dass Personen keine riskanten Kombinationen aus Zugriffsrechten zugewiesen werden, die es ihnen ermöglichen könnten, bei Verwendung der Systeme, die sie benutzen dürfen, betrügerische Handlungen vorzunehmen.

Prozessbeschreibung

Der „Evaluate Violation"-Prozess bedient sich der im „Create New Constraint Policy"-Prozess niedergelegten Regeln, um festzustellen, ob ein und derselben Person riskante Kombinationen von Zugriffsrechten gewährt wurden. Dabei werden auch Verstöße aufgedeckt. Manager können die Situation danach analysieren, ob sie hier eine Genehmigung erteilen oder verwehren sollten.

Best-Practice-IGA-System-Funktionalität

Das IGA-System prüft Benutzer- Identitäten auf Verstöße; wird ein Verstoß aufgedeckt, sendet ein Workflow dem Manager die Aufgabe, diesen zu genehmigen. Genehmigt der Manager den Verstoß durch Hinzufügen von Anmerkungen und Auswahl eines ausgleichenden Kontrollmechanismus, wird der Zugriff nach Genehmigung durch die Sicherheitsbeauftragten bereitgestellt. Wird der Verstoß allerdings nicht genehmigt, wird kein Zugriff bereitgestellt.

Erkennt das IGA-System das Vorhandensein eines Verstoßes, weil eine neue SoD-Regel hinzugefügt wurde, widerruft es keinen Zugriff, da dies die betrieblichen Abläufe behindern könnte, sondern übersendet dem Manager eine Aufgabe, den Verstoß zu genehmigen. Der einen Verstoß darstellende Zugriff wird entfernt, wenn der Manager den Verstoß ablehnt.

Technischer Prozessablauf

1. Die Evaluierung von Identitäten erfolgt zur Feststellung potenzieller riskanter Ressourcenkombinationen auf Basis der SoD-Beschränkungen.
2. Kommt es zur Entdeckung eines Verstoßes, weil einer Person kurz zuvor eine Ressource zugewiesen wurde, wird der Zugriff nicht bereitgestellt, bis der Verstoß entweder genehmigt oder gelöst ist.
3. Ist ein festgestellter Verstoß auf eine bereits vor Erstellung der neuen Einschränkung erfolgte Zuweisung zurückzuführen, ergeht keine sofortige Deprovisionierungsaufgabe. Das IGA-System schiebt weitere Maßnahmen auf, bis der Verstoß genehmigt oder gelöst wird.
4. Dem Manager wird die Aufgabe zugewiesen, den Verstoß zu genehmigen. Hierfür ist allerdings ein Grund anzugeben und ein kompensierender Kontrollmechanismus auszuwählen.
5. Dem Sicherheitsbeauftragten der Benutzergruppe wird die Aufgabe zugewiesen, den Verstoß zu genehmigen. Sie können sich nicht über die Entscheidung des Managers hinwegsetzen, die Aufgabe aber ablehnen und sie mit einem Kommentar an den Manager zurückgeben.
6. Genehmigte riskante Kombinationen werden bereitgestellt oder aufrechterhalten, und gelöste, Konflikte auslösende Zuweisungen werden deaktiviert oder deprovisioniert.

Identity- und Access-Governance

PROZESS-STAKEHOLDERS

Für kontinuierliche Governance sind IGA-Team und Eigentümer von Anwendungen zuständig. Sie müssen sicherstellen, dass alle Anwendungen ständig in angemessenem Zustand sind. Die Vorgesetzten in einer Organisation müssen validieren, dass Endbenutzer Zugriff auf diverse Ressourcen erhalten, wenn sie über Rezertifizierungskampagnen dazu aufgefordert werden.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
IGA-Team	Das IGA-Team wird möglicherweise aufgefordert, Berichte für andere Stakeholder wie z. B. Compliance- und Sicherheitsteams zu erstellen.	Das IGA-Team hat umfassendes Wissen zu den im Data Warehouse gespeicherten Daten und ist somit in einer guten Position, um beurteilen zu können, welche Berichte umsetzbar sind.	Rücksprache mit dem Eigentümer von Anwendungen anwendungsübergreifende Attestierungsumfragen durchführen.	Adhoc Berichtserstellung nach geschäftlichen Anforderungen.
Vorgesetzte	Vorgesetzte prüfen die Berichte und bearbeiten Anträge auf Zugriffsprüfung.	Manager müssen sicherstellen, dass den Accounts und Konten ihrer Mitarbeiter die richtigen Berechtigungen zugeordnet sind. Als Vorgesetzte können sie Anträge auf Zugriffe prüfen und Rechte an ihre ihnen zugeordnete Identitäten vergeben.	Keine	Kontinuierliches Reagieren auf durch Eigentümer von Anwendungen gestellte Anträge auf Zugriffsprüfung.
Eigentümer von Anwendungen	Die Eigentümer von Anwendungen setzen Berichte ein, um festzustellen, wer auf ihre Systeme zugreift. Erstellen von Zertifizierungsprogrammen, um den Zugriff von Benutzern zu überwachen und Bearbeitung von Access Reviews für Eigentümer von Ressourcen. Darüber hinaus leiten sie den Account-Ownership-Prozess zur Prüfung verwaister Kontenzuweisungen und deren Übertragung an einen neuen Eigentümer ein.	Die Eigentümer von Anwendungen sind zuständig für die Sicherstellung von Sicherheit und Compliance ihrer Systeme. Daher müssen sie sicherstellen, dass ausschließlich Berechtigte entsprechenden Zugriff erhalten und verwaiste Konten entweder anderen Eigentümern zugewiesen oder deaktiviert werden.	Die Eigentümer von Anwendungen müssen sicherstellen, dass es eine unternehmerische Umsetzung der technischen Rechte gibt, damit Vorgesetzte auf geschäftlicher Ebene auf Zugriffsrechte reagieren können. Darüber hinaus sollten System-Eigentümer spontane oder zeitlich geplante Attestierungsumfragen für ihr System vorsehen.	Kontinuierliches Management der Sicherheit und Compliance der entsprechenden Systeme durch Analyse der Identität der Zugreifenden und Managen verwaister Konten.

Wichtige Best Practices

Empfehlungen

Im Folgenden eine Reihe von Best-Practice-Empfehlungen, die bei der Umsetzung von Governance-Prozessen in IdentityPROCESS+ bedacht werden sollten.

Definieren von Kennzahlen für ein Kritisches Erfolgsfaktoren (KPI)-Modell
Es ist wichtig, zu definieren, welche KPIs gemessen, überwacht und in Berichten aufgeführt werden. Zur Administration des IGA-Systems umfasst dies auch System-KPIs wie freien Datenbankspeicherplatz, Reaktionszeiten und Ressourcennutzung. Zum Monitoring des IGA-Systems aus Unternehmenssicht sind auch Faktoren wie gemanagte Identitäten, Zahl der Zuweisungen und nicht zugeordnete Konten („orphan accounts") zu berücksichtigen. Bei der Betrachtung der erforderlichen KPIs sollten sowohl Stakeholder aus dem betreffenden Bereich als auch Vorgesetzte sowie Compliance-Team und externe Auditoren miteinbezogen werden, da diese noch zusätzliche Anforderungen haben könnten.

Bei der Bearbeitung von KPIs und Berichten sollten Organisationen dringend bei out-of-the-box Optionen der IGA Lösung ansetzen, anstatt das Rad neu zu erfinden und eigene Lösungen auszuarbeiten. Die meisten Organisationen sind der Auffassung, dass die Standardberichte die meisten ihrer Anforderungen abdecken, und müssen daher nur eine kleine Anzahl maßgeschneiderter Berichte erstellen. Die Klärung der Frage, ob verfügbare Standardberichte für die Organisation geeignet sind, könnte bis zu einem Jahr dauern, wenn zahlreiche Stakeholder mit verschiedenen Anforderungen beteiligt sind.

Bestimmung der erforderlichen Art von Rezertifizierungskampagnen
Zur Sicherung verlässlicher Governance ist es wichtig, straff organisierte Zertifizierungskampagnen durchzuführen. Die Häufigkeit von Rezertifizierungskampagnen sollte auf der Kritikalität der Anwendung und aller externen Compliance-Bestimmungen basieren, die ebenfalls zu berücksichtigen sind. So kann z. B. der Zugriff auf eine wichtige Banking-Anwendung alle sechs Monate einer Rezertifizierung bedürfen, wohingegen weniger wichtige Anwendungen wie das Urlaubsplanungssystem der Personalabteilung möglicherweise nur einmal pro Jahr eine Rezertifizierung des Zugriffs braucht. Bei der Bestimmung der Häufigkeit der Rezertifizierung sollte mit dem Audit-Team Rücksprache gehalten werden, das ebenfalls spezifische Anforderungen haben könnte.

Den Ablauf von Umfragen definieren
Zur effektiven Durchführung der Rezertifizierung von Benutzerzugängen sollten Organisationen festlegen, wie Umfragen ablaufen sollen. Dies umfasst auch Angaben über die Eigentümer von Umfragen und darüber wer sie durchführt und bei Nichtbeantwortung nachfasst. In die Entscheidung, wer die Umfragen managt, sollten auch „politische" Erwägungen einfließen – so dürfte beispielsweise eine leitende Führungskraft etwas unfroh darüber sein, wenn sie von einer weniger hochrangigen Führungskraft eine Erinnerungsnachricht zu einer noch unbeantworteten Rezertifizierungs-Umfrage erhält.

Zusammenfassung

Governance-Prozesse ermöglichen Organisationen die Gewährleistung von Compliance bei Benutzer- Identitäten während der gesamten Beschäftigungsdauer. Dadurch können Administratoren kontinuierlich Prüfungen auf verwaiste Konten durchführen und Maßnahmen zur Verhinderung schädlicher Zugriffskombinationen einleiten, die Verstöße gegen die Funktionstrennung (SoD) mit sich bringen.

Zum Monitoring der Compliance muss eine Definition und Messung im Vergleich zu Kritischen Erfolgsfaktoren (KPIs) erfolgen, damit die Unternehmensleitung beurteilen kann, wie gut die IGA-Lösung und mit ihr verbundene Prozesse für Sicherheit und Compliance im Unternehmen sorgen.

Durch Implementierung der Governance-Prozesse von IdentityPROCESS+ schaffen Organisationen Sicherheit und Compliance und können die Gewährung von Zugriffsrechten an Endbenutzer effektiv unterstützen.

Prozessbereich

Administration

Wenn in einer Organisation neue Anwendungen eingeführt werden, müssen diese unbedingt auch ins IGA-System integriert werden, damit Identitäten und die Provisionierung an Benutzer automatisiert ablaufen und zentral gemanagt werden kann. Dies ist nicht nur wichtig, weil es die Effizienz des Identity-Administrators erhöht, sondern auch sicherstellt, dass Policies wie z. B. die Funktionstrennung automatisch durchgesetzt werden.

Administrative Prozesse beinhalten sämtliche Workflows, mit denen eine Organisation neue (Fach-)Anwendungen effektiv einführen und ihnen sinnvolle Beschreibungen zuordnen kann, damit Endbenutzer bei Self-Service-Anfragen alle Ressourcen finden, die sie brauchen. Die administrativen Policies regeln darüber hinaus die Gestaltung von Policies für Vergabe und Zurücksetzen von Passwörtern.

Administration IGA
Bei Einführung einer neuen Business-Anwendung – auch als Zielsystem bezeichnet – in einer Organisation erfolgt deren Integration in das IGA-System mithilfe von administrativen Prozessen.

Bevor Manager und Endbenutzer über Self-Service-Prozesse mit der Beantragung von Ressourcen oder der Genehmigung von Zugriffsanträgen beginnen, sollten die Ressourcen sinnvoll benannt werden, um Benutzern das Auffinden der entsprechenden Anwendungen zu erleichtern und Managern anzuzeigen, worauf sie Zugriff gewähren. Nach Aufsetzen des Systems nutzen die Administratoren die Passwort-Management-Administrationsprozesse des IGA Systems, um die Durchführung von Passwort-Resets und -Authentifizierungen sowie die Umsetzung der allgemeinen Passwortregeln zu ermöglichen. Administrative Prozesse geben Administratoren Workflows an die Hand, mit denen sie Ressourcen im Zielsystem verändern oder Ressourcen, die die Organisation nicht mehr benötigt, löschen können.

Dieser Prozessbereich umfasst die folgenden Prozesse:

Management von Zielsystemen
- Erstellen, Ändern oder Löschen von Ressourcen der Zielsysteme
- Einführung von Anwendungen

Password-Management
- Passwort-Policy-Zurücksetzen nicht authentifizierter Passwörter
- Registrierung von Passwort-Resets
- Zurücksetzen authentifizierter Passwörter

Warum die Administration von Identitäten wichtig ist:

1. Ermöglicht das effiziente Onboarding neuer Geschäftsanwendungen in das IGA-System.
2. Sicherstellen, dass globale Policies wie z. B. die Funktionstrennung (SoD) auch Anwendung auf neue Anwendungen finden.
3. Erleichtert das Einrichten von Passwort-Reset-Management und Passwortregeln.

Prozess

Management von Zielsystemen

Verwaltet die Verbindung des IGA-Systems zu den Zielsystemen, wodurch das IGA-System die Bereitstellung, Änderung und Deprovisionierung von Zugängen zentral steuern kann.

ERSTELLEN, ÄNDERN ODER LÖSCHEN VON RESSOURCEN IM ZIELSYSTEM

Informationen über die Geschäftsanwendungen, die auch als „Zielsysteme“ bezeichnet werden, müssen in das IGA-System importiert und dort verwaltet werden, damit ein Management des Benutzerzugriffs erfolgen kann.

Prozessbeschreibung Onboarding

Durch die Ressourcen-Prozesse für Zielsysteme können Administratoren das IGA-System mit Anwendungen verknüpfen, damit sie Informationen wie z. B. Benutzer-Zugriffsrechte auslesen und neue Zugriffsrechte in Zielsystemen eintragen können.

Diese Anfangsdaten werden so angereichert, dass das IGA-System bei der Implementierung von Prozessen und Regeln noch effizienter funktioniert. Werden Ressourcen des Zielsystems außer Betrieb genommen, können sie aus dem IGA-System entfernt werden.

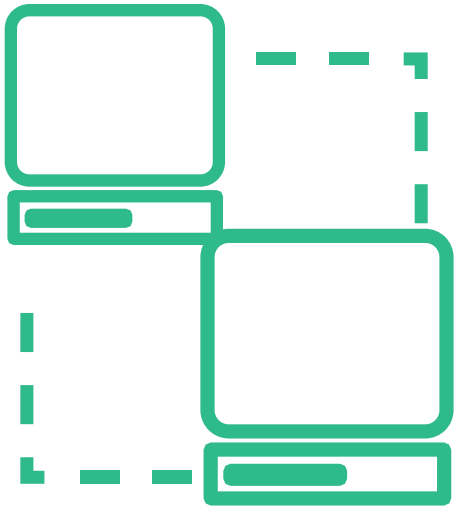
Best-Practice-IGA-System-Funktionalität

Die Ressourcen des Zielsystems werden über Datensammelschnittstellen von verbundenen Systemen in das IGA-Daten-Warehouse eingelesen. Dann werden alle Ressourcen im IGA-Server erstellt.

Jede Zielressource muss zusätzlich angereichert werden, um Daten über Eigentumsverhältnisse, Anzeigen/Verbergen von Zugriffsanträgen, Status und Gültigkeit, Attribute, genehmigte Levels, Delegierung, Exklusivverwaltung und Gültigkeitszustand zu enthalten. Nach Abschluss dieser Anreicherung kann die Zielsystem-Ressource im IGA-System verwaltet werden.

Technischer Prozessablauf

1. Zielsystem-Ressourcen werden in das IGA-System eingelesen.
2. Die Ressourcen werden ins Data-Warehouse übertragen.
3. Auf dem Server werden Ressourcen erstellt oder der Onboard-Applikation-Prozess verwendet, um im Server Ressourcen im Zielsystem zu erstellen.
4. Der Administrator oder System- bzw. Ressourcen-Eigentümer reichert die Daten im IGA-System an.



ONBOARDING EINER APPLIKATION

Dies beinhaltet die Definition von logischen Applikationen in OIS, die Zuordnung von physischen Zielsystemen und das Management von entsprechenden Applikationsrollen.

Geschäftsanwendungen benötigen oftmals Zugriff zu diversen Funktionalitäten in der Anwendung, die Endbenutzern nicht bekannt sind. Die Definition einer Endbenutzer-Anwendung muss vereinfacht werden, damit alle im Hintergrund vorhandene Komplexität verborgen bleibt. Dadurch können Benutzer einfach und schnell benötigte einzelne Anwendungen auswählen, ohne dass dafür ein Verständnis der technischen Details erforderlich wäre. Dies reduziert nicht nur die zur Zugriffsbeantragung benötigte Zeit, sondern auch die Fehlerwahrscheinlichkeit bei der Genehmigung durch Manager.

Prozessbeschreibung

Jede Anwendung kann aus diversen Zielsystemen bestehen. So kann z. B. eine Anwendung, die zur Zugriffskontrolle Active Directory einsetzt, aus der Anwendung selbst und Active Directory bestehen.

Die Systeme, aus denen eine Anwendung besteht, werden definiert; die Anwendung wird dann sinnvoll benannt und beschrieben. Diese Benennungen und Beschreibungen sollen zum einen Endbenutzern das Auffinden von Anwendungen erleichtern, zu denen sie Zugriff beantragen wollen und zum anderen für Manager nachvollziehbar machen, was sie genehmigen.

Best-Practice-IGA-System-Funktionalität

Der Administrator definiert die logischen Anwendungen im IGA-System auf Basis der hierfür erforderlichen Zielsysteme und deren Ressourcen.

Als nächstes werden die Anwendungsrollen durch aussagekräftige Business-Beschreibungen und andere Attribute aufbereitet, die Endbenutzern ermöglichen, diese bei Service-Anfragen zu finden.

Beschreibung und Daten der Anwendung werden von einem Onboarding-Administrator überprüft und genehmigt und dann vom IGA-System für den Access-Request-Prozess verfügbar gemacht.

Technischer Prozessablauf

1. Der IT-Eigentümer der Anwendung leitet den Prozess ein und wählt das System aus.
2. Der IT-Eigentümer definiert die verbundenen physischen Systeme.
3. Der IT-Eigentümer definiert bei Bedarf auch andere Eigentümer.
4. Der IT-Eigentümer wählt die in der Anwendung zu verwendenden anderen Anwendungen beim IGA-Server oder Data Warehouse aus.
5. Der Business-Owner gestaltet die Anwendungsrollen.
6. Der Business-Owner kann bei Bedarf auch andere Business-Owner festlegen.
7. Ein Anwendungs-Onboarding-Administrator genehmigt die Änderung von Anwendung und Rollen.

Prozess

Password-Management

Ermöglicht Organisationen das Management von Passwortregeln für jede Fachanwendung und lässt Benutzer ihre eigenen Passwörter sicher zurücksetzen.

PASSWORTREGELN

Die Passwortregeln für jede angebundene und gemanagte Fachanwendung müssen der Stärke des Passworts entsprechen, die für das jeweilige System verlangt werden. Es sind Passwortregeln zu erstellen, um sicherzustellen, dass eine Mindeststärke von Passwörtern gegeben ist, die systemübergreifend für Sicherheit sorgt.

Prozessbeschreibung

Dieser Prozess stellt sicher, dass die Generierung von Passwörtern im IGA-System Passwörter hervorbringt, die den Anforderungen an die Fachanwendung entweder gleichwertig sind oder sie sogar übertreffen.

Best-Practice-IGA-System-Funktionalität

Die Passwortregeln werden für jede Fachanwendung so beschrieben, dass Endbenutzer sie nachvollziehen können und klar ist, welche Zeichen verwendet werden können und wie lang das Passwort sein muss. Die Daten-Administratoren definieren im IGA-System Passwortregeln, um Policies für die Mindeststärke von Passwörtern festzulegen. Bei Bedarf kann ein System-Eigentümer auch die Passwortregeln der Zielsysteme, für die er zuständig ist, ändern, um die Systemsicherheit zu gewährleisten.

Technischer Prozessablauf

1. Prüfung der bestehenden Passwortregeln für Systeme, in denen Passwörter zu generieren sind.
2. Für jedes System Passwortregeln festlegen, die die Vorgaben des Zielsystems erfüllen oder übertreffen.
3. Erstellen von Passwortregel-Beschreibungen, um Benutzer bei der Erstellung von Passwörtern zu unterstützen.
4. Datenverantwortliche können im IGA-System Passwortregeln erstellen und pflegen.
5. System-Eigentümer können ihren Zielsystemen geeignete Passwortregeln zuweisen.

ZURÜCKSETZEN VON PASSWÖRTERN

Benutzer brauchen eine schnelle, effiziente und sichere Methode zum Reset vergessener Passwörter, ohne hierzu das Helpdesk kontaktieren zu müssen.

Prozessbeschreibung

Benutzer, die ihr Passwort vergessen haben, können den Reset mit einem Self-Service-Prozess durchführen, ohne das Helpdesk des Unternehmens zu nutzen. Dabei beantwortet der Benutzer bestimmte Fragen, deren Antworten er zu einem früheren Zeitpunkt eingegeben hat. Beantwortet er die Fragen richtig, darf er ein neues Passwort erstellen.

Best-Practice-IGA-System-Funktionalität

Nachdem der Benutzer einen Benutzernamen im Self-Service-Passwort-Portal eingegeben hat, prüft das IGA-System, ob es sich um eine aktive Identität handelt. Dann muss der Benutzer mehrere persönliche Fragen richtig beantworten. Werden diese Schritte erfolgreich durchgeführt, gibt der Benutzer ein Passwort ein.

Das IGA-System prüft, ob das neue Passwort die Passwortregeln erfüllt und erstellt einen Provisionierungsantrag zur Durchführung der Resets.

Technischer Prozessablauf

1. Ein Benutzer, der sich wegen vergessenem Passwort nicht einloggen kann, loggt sich beim Self-Service-Passwortportal ein und gibt einen Benutzernamen ein. Der Benutzername muss einer aktiven Identität zugeordnet sein.
2. Der Benutzer beantwortet eine zuvor festgelegte Anzahl persönlicher Fragen, die er bei der Registrierung ausgewählt hat.
3. Der Benutzer gibt ein neues Passwort ein, dass die Vorgaben der Passwortregeln erfüllen oder übertreffen muss.
4. Das Passwort wird in den für einen Reset freigeschalteten Zielsystemen zurückgesetzt.
5. Dem Eigentümer der technischen Identität wird mitgeteilt, ob der Prozess erfolgreich war oder eine Fehlermeldung erzeugt hat.

REGISTRIERUNG FÜR PASSWORT-ZURÜCKSETZUNG

Die persönlichen Fragen werden eingesetzt, um sicherzustellen, dass Vorgänge beim Self-Service-Passwort-Reset sicher ablaufen; hierzu vergewissert man sich der Tatsache, dass der Benutzer auch wirklich die Person ist, die sie vorgibt zu sein.

Prozessbeschreibung

Der Registrierprozess für Passwort-Zurücksetzung gestattet dem Administrator die Bearbeitung persönlicher Fragen, die einem Benutzer zur Verfügung stehen, wenn er sein Passwort zurücksetzen möchte. Diese Fragen sind z. B. vom Typ „Wie lautet der Mädchenname Ihrer Mutter?“ oder „Welche Farbe hatte Ihr erstes Auto?“. Das IGA-System setzt diese vordefinierten, persönlichen Fragen beim Zurücksetzen von Passwörtern ein, um sicherzustellen, dass der Benutzer auch wirklich die betreffende Person ist.

Best-Practice-IGA-System-Funktionalität

Die IGA-Lösung bietet eine Liste von vordefinierten Fragen an. Aus diesen kann der Administrator bzw. der jeweilige Endbenutzer einige auswählen, die für das spätere Entsperren verwendet werden. Der Administrator kann darüber hinaus Passwortregeln festlegen, z.B. die Länge der Passwörter, Notwendigkeit von Ziffern oder Sonderzeichen sowie die Anzahl möglicher Reset-Fehlversuche vor Sperrung der Identität.

Hat der Endbenutzer sich für das Zurücksetzen des Passwortes über Self-Service registriert, werden ihm eine Reihe persönlicher Fragen gestellt, die er richtig beantworten muss, damit er den Reset ausführen kann.

Technischer Prozessablauf

1. Der Administrator wählt die vordefinierten Fragen aus, die Benutzer beantworten sollen.
2. Bei Bedarf arbeitet der Administrator neue Fragen aus.
3. Der Administrator definiert Parameter wie z. B. die Zahl der zu beantwortenden Fragen und die Zahl von Fehlversuchen beim Reset, nach denen die Identität gesperrt wird.

ZURÜCKSETZEN VON PASSWÖRTERN

Da es sinnvoll ist, regelmäßig das Passwort zu wechseln, benötigen Benutzer eine schnelle, effiziente und sichere Methode, um vorhandene Passwörter ohne Unterstützung durch das Helpdesk zu ändern. Manager oder Administratoren können auch bestimmen, dass Benutzer ihr Passwort ändern sollten, beispielsweise bei Verdacht auf missbräuchliche Verwendung von Passwörtern.

Prozessbeschreibung

Durch diesen Prozess können Benutzer Passwörter im Self-Service-Verfahren zurücksetzen, ohne hierzu das Helpdesk kontaktieren zu müssen.

Best-Practice-IGA-System-Funktionalität

Der Manager oder operative Administrator wählt die Personen aus, deren Passwort im IGA-System zurückgesetzt werden sollten; dem Benutzer wird eine Liste von Identitäten vorgelegt, die nach Passwortregel geordnet sind; im zugrundeliegenden System ist die Möglichkeit zur Passwort-Zurücksetzung aktiviert.

Das IGA-System fordert den Benutzer zur Eingabe des bisherigen und neuen Passworts auf. Das IGA-System prüft, ob das neue Passwort die Passwortregeln erfüllt und erstellt einen Provisionierungsantrag zur Durchführung einer Synchronisation.

Technischer Prozessablauf

1. Der Manager oder operative Administrator leitet den Prozess des Passwort-Rücksetzens ein.
2. Der Benutzer wählt die Konten aus, die er zurücksetzen möchte.
3. Das neue Passwort, das die Passwortregeln erfüllen oder übertreffen muss, wird eingegeben.
4. Das Passwort wird für die ausgewählten Konten zurückgesetzt.

! BEST PRACTICE...

Durch die Bereitstellung der Passwort-Self-Service-Funktionen wird das Helpdesk deutlich entlastet.

Administration

PROZESS-STAKEHOLDERS

Die administrativen Prozesse in IdentityPROCESS+ umfassen das Management von Zielsystemen, Anwendungen und Passwörtern. IGA-Team und Eigentümer von Anwendungen sind zuständig für diese Prozesse, in denen Endbenutzer mit dem IGA-System interagieren, wenn diese ihr Passwort zurücksetzen müssen.

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
IGA-Team	Das IGA-Team managt die Zielsystem-Ressourcen im IGA-System.	Das IGA-Team ist zuständig für das Management der Zielsystem-Ressourcen im IGA-System. Es stellt deren korrektes Funktionieren sicher. Die IGA-Administratoren erstellen die für Endbenutzer erforderlichen, vordefinierten Fragen zur Authentifizierung der eigenen Person vor Durchführung eines Resets, falls diese ihre Passwörter vergessen haben.	Verbindung von Zielsystemen mit dem IGA-System.	Kontinuierliches Management der Zielsysteme im IGA-System, einschließlich Entfernung von Zielsystemen, wenn diese nicht mehr aktiv in Benutzung sind.
Endbenutzer	Endbenutzer interagieren beim Zurücksetzen ihrer Passwörter mit dem IGA-System.	Endbenutzer müssen eventuell ihr Passwort zurücksetzen – weil sie es vergessen haben oder weil der System-Eigentümer sie in regelmäßigen Abständen dazu auffordert.	Keine	Keine
Eigentümer von Anwendungen	Die Eigentümer von Anwendungen müssen sicherstellen, dass angereicherte Daten den Zielsystemen hinzugefügt werden und festlegen, welche Ressourcen im Zielsystem Endbenutzer-Anwendungen definieren.	System-Eigentümer können definieren, welche Genehmigungslevels erforderlich sind, ob Zugriff delegiert werden kann und welche Passwortstärken erforderlich sind. Zusammenarbeit mit dem IGA-Team, um sicherzustellen, dass Änderungen im Zielsystem – wie z. B. API-Upgrades oder -Änderungen – die Konnektivität zur IGA nicht beeinträchtigen.	Definieren, aus welchen Zielsystemen die Endbenutzeranwendungen bestehen sollen.	Kontinuierliche Rezertifizierung von Anwendungsrollen, um sicherzustellen, dass die hier zugrundeliegenden Zielsysteme noch gültig sind.

Wichtige Best Practices

Empfehlungen

Im Folgenden eine Reihe von Best-Practice-Empfehlungen, die bei der Implementierung administrativer Prozesse in IdentityPROCESS+ bedacht werden sollten.

Anreichern der Ressourcen im Zielsystem
Obwohl das IGA-System Informationen aus dem Zielsystem bezieht, sollten System- und Ressourcen-Eigentümer auch noch alle verfügbaren Zusatzinformationen hinzufügen, um einen effektiven Ablauf der Prozesse zu gewährleisten. Hierzu zählen u.a. Angaben über die Eigentümerschaft des Zielsystems, ob Zugriffsanträge angezeigt oder verborgen werden sollten, welche Genehmigungslevels zur Genehmigung von Zugriff zur jeweiligen Ressource erforderlich sind sowie Angaben zur Frage, ob der Benutzer-Zugriff auch an andere delegiert werden kann.

Regelmäßige Rezertifizierung von Definitionen der Anwendungsrollen
Anwendungen und die ihnen zugrunde liegenden Ressourcenanforderungen ändern sich im Laufe der Zeit, da Systeme geändert und aktualisiert werden. Um sicherzustellen, dass Rollendefinitionen in Anwendungen korrekt sind, sollten Organisationen hier regelmäßige Rezertifizierungen durchführen, um Ressourcen-Eigentümern die Möglichkeit zu geben, Informationen über Zielsysteme zu aktualisieren.

Passwortregeln
Bei der Erstellung von Passwortregeln sollte auf eine ausreichende Komplexität geachtet werden. Eine Passwortregel sollte zumindest fordern, dass sowohl Groß- als auch Kleinschreibung und Zahlen zu verwenden sind. Unterstützen die Zielsysteme auch Sonderzeichen, sollte die Passwortregel auch deren Verwendung fordern, da dies die Sicherheit weiter erhöht.

Im Themenbereich Administration zu erwägende Fragen

- Welche Genehmigungslevels sind erforderlich, um im jeweiligen Zielsystem Benutzerzugang zu gewähren?
- Lassen sich Zugangsrechte für einzelne Zielsysteme delegieren?
- Welche Anforderungen bestehen im jeweiligen Zielsystem an die Mindeststärke von Passwörtern?

Zusammenfassung

Die administrativen Prozesse sichern ein reibungsloses Onboarding von Anwendungen, damit diese auch in das IGA-System integriert werden können. Außerdem erlauben sie Administratoren die Vereinfachung von Self-Service-Zugriffsanträgen, da Zielsysteme in einer Anwendung zusammengefasst werden können, die für die beantragenden Endbenutzer und die genehmigenden Manager gut nachvollziehbar sind.

Darüber hinaus zeigt das Managen von Passwortregeln und Reset-Verfahren, dass Organisationen ihre eigene Sicherheit im Griff haben und Benutzern schnelle, effiziente Prozesse zum Reset von deren Passwörtern an die Hand geben können.

Prozessbereich

Auditing

Effektive Audit-Prozesse liefern Reporting-Funktionen sowie operative und Management-Dashboards für Szenarien in den Bereichen Identity Management und Access-Governance. Dies macht Risiken für IT-Auditoren nachvollziehbar und lässt sie Kontrollen einführen, bestehende Risiken bewerten und überprüfen sowie evtl. Korrekturmaßnahmen ergreifen. Beispiele für entsprechende Kontrollen: verwaiste Konten, „Entitlement Creep“ (schleichende Ausweitung von Zugriffsrechten), Verstöße gegen SoD sowie Transparenz bzgl. privilegierter Benutzerkonten.

Hoch entwickelte Auditing-Prozesse liefern auf der Basis von Identity Intelligence einen umfassenden Überblick über system- und anwendungsübergreifend zusammengefasste, geschäftskritische Daten. Identitäten - und Zugriffsdaten werden abgeschottet und mit Policies verglichen. Evtl. unangemessene Zugriffsrechte oder SoD-Verstöße werden automatisch identifiziert und ermöglichen die sofortige Umsetzung von Korrekturmaßnahmen.

Reporting, Analyse und Gegenmaßnahmen mit Blick auf Ist- versus Soll-Zustand
Analyse- und Reporting-Funktionen liefern Übersichten über Identitäten und beantworten die grundlegenden Fragen „wer greift auf was zu?“ und „wer hat den Zugriff genehmigt?“ Beim Auditing-Prozess vergleicht man Policies, Accounts, Berechtigungen, Funktionstrennung (SoD) sowie privilegierte Konten mit dem Ist-Zustand von Identitäten und Zugriffsrechten, weist die Eigentümer von Systemen und Kontrollmechanismen auf Ausnahmen hin und unterstützt eine zügige und geordnete Problembehebung. Validierung des zu erwartenden Status von Business-Policies im Vergleich zum Ist-Zustand von Zugriffsrechten in gemanagten Anwendungen und Systemen mit Warnmeldungen für Administratoren, System-Eigentümer und Sicherheitsbeauftragte bei allen Objekten oder Vorkommnissen mit Handlungsbedarf.

Prozesse im Bereich Auditing:

- Audit Trail
- Audit-Historie
- Audit-Protokoll
- Audit-Policies
- Audit Response

Warum Auditing wichtig ist:

1. Zur Unterstützung der Erstellung und Bewertung von Business-Policies, Regeln und Governance-Kontrollmechanismen.
2. Monitoring der Effektivität von IGA-Prozessen.
3. Gewissheit für Auditoren und Executive Stakeholders, dass geeignete Sicherheits-Regeln und -Policies tatsächlich umgesetzt werden.
4. Ermöglicht der Organisation den Nachweis, dass das IT-Umfeld unter Kontrolle ist und ordnungsgemäß gemanagt wird.

Prozess

Audit Trail

Die Funktion Audit Trail zeigt dem Auditor, warum Zugriff besteht, wer genau ihn gewährt hat und wie dieser Zugriff entstand. Alle Kunden sind in der einen oder anderen Form Compliance-Regelungen unterworfen. Am offensichtlichsten ist dies bei Kunden in regulierten Branchen oder ISO-zertifizierten Organisationen. Sie sollten mit geplanten und spontanen Sicherheits-Prüfungen umgehen können, um die zuständigen Teams kontinuierlich zu überwachen und bei Bedarf zu alarmieren, wenn gegen Regeln verstoßen oder die Sicherheit potenziell gefährdet wird.

CIOs und CISOs müssen sicherstellen, dass Sicherheits-Policies eingehalten werden. Sie müssen imstande sein, Nachweise für die Fähigkeit zum Schutz sensibler Daten vorzulegen sowie kontinuierlich sicherstellen, dass die Organisation sich system- und anwendungsübergreifend an alle Compliance-Vorgaben hält.

Die Audit Trail stellt für Auditoren ein zentrales Feature dar, da sie Prozesse zur Dokumentierung folgender Aspekte enthält:

- Audit Trail für alle Identitätsentscheidungen.
- Audit Trail für verwaltete Identitäten, um festzustellen, warum Zugriff gewährt wurde und wer die Genehmigung erteilt hat.
- Audit Trail für verwaltete Identitäten, die umgangen wurden, um festzustellen, warum vom wem Zugriff erteilt wurde.

Prozessbeschreibung

Die Audit Trail liefert ein detailliertes Reporting über Entscheidungen, die sich auf Berechtigungs-Zuweisungen ausgewirkt haben. Audit Trail umfasst Filter, Such- und Sortier-Funktionen sowie einen Drilldown zu detaillierten Berichten über bestimmte Berechtigungs-Zuweisungen.

Die Audit Trailn-Reporting und -Analysefunktion enthüllt alle ggf. inkorrekt zugewiesenen Zugriffsrechte oder Verstöße gegen die Funktionstrennung (SoD) und liefert die Antwort auf die Frage, wie, warum und wann der Verstoß konfiguriert und/oder genehmigt wurde. Sämtliche Entscheidungen in Zusammenhang mit der Zuweisung von Identitätsberechtigungen werden getrackt und sind im betreffenden Bericht nachzulesen. Die bei Zugriffsgenehmigungen, Rezertifizierungsumfragen und SoD-Reviews gegebenen Antworten werden allesamt aufgezeichnet und stehen für die Reporting-Funktion zur Verfügung.

Best-Practice-IGA-System-Funktionalität

Eine IGA-Lösung sollte eine kontinuierlich hohe Zahl an Buchungskontroll-Daten mit umfassenden Informationen zu folgenden Bereichen enthalten: Objekt- und Genehmigungsänderungen, Zugriffsanträge, Genehmigungen und benutzerdefinierte Objekte. Dieses Funktionalitäts-Level ist von großer Bedeutung für Auditoren und Stakeholder, die sofortige Transparenz bei Zugriffsrechten benötigen und imstande sein müssen, sämtliche Aspekte ihrer Gewährung (wie, wann, warum?) zu dokumentieren, einschließlich aller Aktivitäten bei Zugriffsgenehmigungen, Rezertifizierungs-Umfragen und SoD-Reviews.

Technischer Prozessablauf

1. Ein Mitarbeiter versendet einen Antrag auf Zugriff unter Nennung des Grundes; der Antrag wird aufgezeichnet.
2. Der Antrag auf Zugriff wird sowohl vom Manager als auch vom Ressourcen-Eigentümer genehmigt; die Antworten werden aufgezeichnet.
3. Der Zugriff wird gewährt, die Audit Trail wird einschließlich Daten zu Genehmigung, Grund, genehmigender Person (einschließlich deren Rolle) und Zeitstempel erfassen.
4. Die Audit Trail wird erfasst, in ein Data-Warehouse importiert und in Standard-Berichten zur weiteren Analyse und Dokumentierung niedergelegt.
5. Die Audit Trail wird archiviert, um für Verlaufsanalysen zur Verfügung zu stehen

Prozess

Audit Historie

Das Aufzeichnen der Audit Historie ist eine Grundanforderung an das Audit-Reporting und ermöglicht es der Organisation, den vom Auditor geforderten Dokumentationspflichten prompt und effizient nachzukommen. Auditoren sollte Zugriff zu On-Demand erstellten Berichten und unterstützenden Dokumentationen gegeben werden; dies umfasst Verlaufsdaten für Identity Lifecycle-Prozesse, Zugriffsanträge, Kontenänderungen, Berechtigungen und Genehmigungen.

Prozessbeschreibung

Die Audit Historie stellt alle historischen Prozessdaten bereit, die sowohl in on-premises als auch in cloudbasierten Systemen unter dem Management der IGA-Lösung stehen. Historische Daten werden in einem Dashboard angezeigt und sind in verschiedenen Reports für Identitäten, Konten, Ressourcen-Zuweisungen, Policies und Systemen verfügbar.

Verlaufsdaten sollten im Data Warehouse der IGA-Lösung gesammelt, gespeichert und entsprechend archiviert werden. Daraus ergibt sich die Möglichkeit zur Anzeige eines kompletten Überblicks mit Compliance-relevanten Statistiken. Der Prozess sollte eine spezielle Datums-/Zeitstempel-Funktionalität zur jederzeitigen Dokumentation spezifischer Aktionen enthalten. Hoch entwickelte historische Auditing-Funktionen umfassen: Zeitpunkt, Änderungen in einer bestimmten Periode, historische Entwicklung sowie Change-Log-Reporting.

Best-Practice-IGA-System-Funktionalität

Jedes Objekt im IGA-System sollte es dem Auditor ermöglichen, Suchumfang und Parameter zu definieren; diese können sein: Gültigkeitsdauer und -daten, Status, Kategorien sowie Nutzungsmuster auf Basis ausgewählter Werte wie z. B. Identitäten, Kontexte, Konten, Ressourcen und deren Zuweisungen, verwaiste Objekte, Kontennutzung, Daten-Qualität und Systeme. Die Daten werden aus dem IGA-Data-Warehouse extrahiert und archiviert, um Berichte zu generieren.

Die Generierung von Dashboards und maßgeschneiderten Reporting-Frameworks ist individuell konfigurierbar. Daten sollten zur weiteren Analyse in zahlreiche Formate exportierbar sein.

Technischer Prozessablauf

1. Der Status des Datenobjekts wird gespeichert und ist im Data Warehouse verfügbar.
2. Jeder Objekttyp – z. B. Konten und Berechtigungen –, der in das Data Warehouse importiert wird, wird als Slowly Changing Dimension (SCD) mit einer Darstellung des Verlaufs des Objektstatus abgebildet.
3. Änderungen des Objektstatus werden beim Vergleich von importierten Objekten mit bereits in der Data-Warehouse-Datenbank gespeicherten Objekten festgestellt. Der Vergleich von Objekten erfolgt auf Attribut-Ebene.
4. Ändert sich das Status-Attribut eines Objekts, erstellt das Data-Warehouse eine neue Version des Objekts mit neuem Versionswert.
5. Der Verlauf eines Objekts setzt sich aus allen getrackten Versionen zusammen. Jede Version steht für den Objektstatus zu einem bestimmten Zeitpunkt, angezeigt durch eine Gültigkeits- und Ablaufzeit
6. Historische Daten aus dem Data-Warehouse werden zum Auditing-Reporting auf dem Dashboard angezeigt.

Prozess

Audit-Protokoll

Zum Nachweis, dass eine Organisation die geeigneten Maßnahmen für das Access-Monitoring und die Sicherstellung der Einhaltung gesetzlicher Bestimmungen trifft, müssen alle Umfrage-Audits protokolliert werden, um dem Auditor zu versichern, dass geeignete Kontrollmechanismen bestehen.

Prozessbeschreibung

Auditor, Systemadministrator und die betreffenden System-Eigentümer können zugewiesene Umfragen-Audits ansehen, sie in Echtzeit aktualisieren sowie Berichte zur kontinuierlichen Bewertung von wichtigen Kontrollen, Geschäftsregeln, Datenintegrität und Leistung überprüfen.

Der Auditor sollte imstande sein, zu prüfen und nachzuweisen, dass ein Umfrage-Audit unter Wahrung der Sicherheitsanforderungen, gesetzlichen Kontrollen und Business-Policies stattgefunden hat. Eventuelle Korrekturmaßnahmen sind mit Datum und Uhrzeit zu protokollieren.

Best-Practice-IGA-System-Funktionalität

Auditoren, Datenschutzbeauftragte (DPOs) oder Systemadministratoren erhalten über das IGA-Portal eine Dashboard-Ansicht. Auf Basis der Systemadministrations-Ansicht ermöglicht das Dashboard Auditoren oder Administratoren die konstruktive Nutzung verschiedener Widgets zum Anzeigen von Informationen aus Quellen wie z. B. Event Viewer, Anwendungsprotokollen, IGA- und SQL- Prozessen etc.

Technischer Prozessablauf

1. Auditor oder IGA-System-Eigentümer können sich alle im IGA-System durchgeführten Compliance-Umfragen anzeigen lassen.
2. Auffinden der Umfrage, für die zusätzliche Informationen erforderlich sind
3. Echtzeit-Durchsicht der gewünschten Umfrage.
4. Möglichkeit zur Nachbearbeitung von Antworten und Export in ein PDF.
5. Wiederholen Sie den Prozess für alle Umfragen, für die dieses Informationslevel gefordert ist.

Prozess

Audit-Policies

In der Regel werden Audit-Policies mit den Geschäftsregeln einer Organisation abgestimmt und dann in die jeweiligen IGA-Prozesse eingegliedert. Audit-Policies sollten routinemäßig geprüft werden, um sicherzustellen, dass sie Maßnahmen effektiv umsetzen und die gewünschten unternehmerischen Ergebnisse erzielen. Um die kontinuierliche Einhaltung von Regeln und Datenintegrität zu gewährleisten, sollte die Organisation über die zentralen, in die IGA-Prozess eingebauten Kontrollen hinaus noch weitere Audit-Policies nutzen.

Prozessbeschreibung

Audit-Policies vergleichen Geschäftsregeln und Kontrollmechanismen mit dem Ist-Zustand von Identitäten und verbundenen Zugriffsrechten. Bei Entdeckung von Unstimmigkeiten oder Verstößen sollte der Prozess auch eine Methode enthalten, die Kontroll-Eigentümer warnt und ihnen die Umsetzung von Korrekturmaßnahmen ermöglicht.

Der Prozess umfasst auch eine Funktion zum Policy-Management über ein Auditing-Dashboard, das alle Audit-Policies anzeigt, die ein bestimmter Benutzer ansehen und managen darf.

Best-Practice-IGA-System-Funktionalität

Audit-Policies sollten so konfiguriert sein, dass kontinuierlich alle aktiven Identitäten geprüft und der Ist- mit dem Soll-Zustand verglichen wird. Dieser Vergleich bringt alle evtl. vorhandenen Unstimmigkeiten zur Kenntnis der geeigneten Support-Teams, wie z. B. technische Konten ohne Eigentümer, Externenzugriff mit fehlendem oder ungültigem Ablaufdatum, Rollen mit konfliktgeladenen Berechtigungen oder Verstöße im Rahmen von Segregation of Duty-Kombinationen bzw. nicht in Rezertifizierungsumfragen enthaltene Berechtigungen.

KONTROLL-POLICIES

Werden kontinuierlich eingesetzt, um Unstimmigkeiten in Policies zu entdecken und darauf zu reagieren. Potenzielle Probleme: u.a. Objekte ohne Eigentümer, Zirkelbezüge in der Rollenhierarchie, ungeeignet beschriebene Rollen sowie Definition von Pflichtfeldern. Wird in einer Policy ein Problem entdeckt, wird ein Audit-Case-Workflow eingeleitet und dem Policy-Eigentümer zur Lösung vorgelegt.

EINSCHRÄNKUNGSREGELN

Werden in der Regel zur Aufdeckung von Konflikten oder Problemen in Policies zur Funktionstrennung (SoD) verwendet. Der Policy-Eigentümer sollte die Möglichkeit haben, Verstöße zu übergehen und anzunehmen, nachdem er einen triftigen Grund für die Notwendigkeit der Implementierung kompensierender Kontrollmaßnahmen angegeben hat. SoD-Ausschlussregeln werden immer dann evaluiert, wenn die Zugriffsrechte für eine Identität in der IGA-Lösung neu evaluiert werden.

RISIKOEINSTUFUNG

Eine Policy zur Definition des Risikos, die fehlerhaft gestaltete Kontroll-Policies und Ausschlussregeln beinhalten. Jede falsch angewandte Policy und jede Umgehung von Ausschlussregeln beeinflusst die Risikoeinstufung.

Prozess

Audit Response

Audit Response-Prozesse ermöglichen der Organisation, dass Ausnahmen sicher festgestellt und vom zuständigen Policy-Eigentümer bearbeitet werden. Dieser kann Korrekturmaßnahmen einleiten.

Prozessbeschreibung
Die IGA-Lösung sollte so konfiguriert werden, dass sie kontinuierlich Policies nach bestimmten Zeitplänen bewertet oder spontan von Audit-Policy-Eigentümern ausgelöst werden kann. Audit Response-Prozesse dienen der Beseitigung von Regelverstößen oder Ausnahmen, die im Zuge einer Policy-Bewertung festgestellt werden.

Regelverstöße sollten als Vorfälle behandelt und über einen Eskalations-Workflow für handlungsfähige Follow-Up- und Korrekturmaßnahmen verfolgt werden.

Best-Practice-IGA-System-Funktionalität
Wird ein Regelverstoß erkannt oder beobachtet, lösen Kontroll-Policies einen Workflow aus, der den Policy-Eigentümer informiert. Teil des Workflows: festzustellen, ob für den betreffenden Verstoß/die Ausnahme bereits ein Vorfall/eine Akte besteht und entscheiden, ob eine neue Akte/ein neuer Vorfall angelegt werden muss.

Der Workflow setzt den Policy-Eigentümer, den Manager des Benutzers oder Informationssicherheitsteams in Kenntnis, denen die besondere Aufgabe obliegt, den geeigneten Ansatz zur Beseitigung des Zwischenfalls zu wählen. Je nach Regelverstoß und erforderlicher Ausnahme kann der Policy-Eigentümer eine Genehmigung erteilen, Korrekturmaßnahmen vornehmen, den Vorfall beheben oder den Vorgang abschließen.

Technischer Prozessablauf

1. Daten aus Zielsystemen werden in das Data-Warehouse geladen. Verlauf und Verbesserungen von KPIs werden überwacht.
2. Konten werden mit Identitäts-Stammdaten abgeglichen und zur Risikobewertung zu einer plattformübergreifenden Identitäts-Ansicht konsolidiert.
3. Statusänderungen erkennt man durch Vergleich importierter Identitätsdaten mit den gespeicherten Daten. Relevante Ausnahmen werden sofort in den Dashboards für Auditberichte angezeigt.
4. Bei einer Statusänderung wird ein Ausnahmealarm ausgelöst.
5. Der Policy-Eigentümer erhält Alarmmeldungen mit einer Ausnahmeliste.
6. Der Policy-Eigentümer stellt fest, ob die Ausnahme neu oder bereits bekannt ist und öffnet dann entweder einen neuen Fall oder genehmigt die Ausnahme.
7. Der Policy-Eigentümer analysiert die Ausnahme und entscheidet auf Grundlage der verbunden Audit-Control-Policies, ob Daten einer Korrektur, Mitigation oder einem Update unterzogen werden. Möglichkeit zur Anwendung automatisierter Ausnahme-Migrationsprozesse.
8. Ausnahmen und Maßnahmen werden im Data Warehouse protokolliert, um den Verlauf zu dokumentieren.

Auditing

PROZESS-STAKEHOLDERS

Die Auditing-Prozesse in IdentityPROCESS+ bieten solide Auditing-Funktionen zum Management von Policies, Vorgehen bei Ausnahmen sowie zur Sicherstellung umfassender Audit Trails und Audit Historie und hoch entwickelte Reporting- und Analysefunktionen. Für Handling, Maintenance, Reporting und Analysen in Zusammenhang mit den Prozessen sind in der gesamten Organisation diverse Stakeholder erforderlich:

Stakeholder	Beteiligung	Warum sind sie beteiligt?	Aufgaben vor der Implementierung	Aufgaben nach der Implementierung
Unternehmensführung (CIO, CISO, CPO)	Kommunizieren IGA-relevanter IT-Sicherheitsanforderungen und -ziele	Ausarbeitung einer Zielstellung zum Umsetzen der Auditianforderungen	Keine	Prüfung der Ergebnisse, um sicherzustellen, dass Auditanforderungen ordnungsgemäß festgeschrieben werden
Policy-Eigentümer	Stellt sicher, dass die Policy im Einklang mit den Unternehmenszielen steht, um die angestrebten Resultate zu erzielen	Eigentümer der Policies für den jeweiligen Fokusbereich	Übermittlung der geschäftlichen Anforderungen an das Projektteam	Mitwirkung an Gestaltung von Follow-Up-Maßnahmen für Reporting und Rezertifizierungs-Kampagnen. Bestimmt, wer über Ausnahmen entscheidet
Auditor	Führt Audits durch	Definiert Audit-Parameter	Teilnahme an der Prüfung von Audit-Funktionen	Analysiert und löst Ausnahmefälle
IGA-Team	Konfigurieren und Monitoring der IGA-Plattform	Installieren und Konfigurieren der IGA-Plattform	Sicherstellen der Berücksichtigung sämtlicher IGA-Voraussetzungen	Überwachung und Durchführung von Änderungen an der Plattform

Empfehlungen

Definiert effektive Audit-Prozesse
IEs ist von essenzieller Bedeutung, dass Audit-Policies mit geschäftlichen Abläufen abgestimmt werden und die erwarteten Ergebnisse erzielen. Audit-Prozesse sollten stets Antworten auf folgende Fragen liefern: „Wer greift auf was zu? Wer hat diesen Zugriff bzw. diese Ausnahmeregel genehmigt?“ Die Anwendung von Kontroll-Policies, um Unstimmigkeiten in Policies zu entdecken und darauf zu reagieren. Bereithalten eines Lösungs-Workflows, um alle in den Policies erkannten Probleme zu beheben. Nutzung von Ausschlussregeln, um Konflikte oder Probleme im Bereich Funktionstrennung (SoD) zu entdecken und Wege zur Dokumentierung von Ausnahmen und Umgehungen von Regeln (kompensierende Kontrollen) bereitzustellen. Jedem Policy-Objekt sollte eine Gewichtung/Punktzahl zugewiesen und ein Risk-Scoring-Kontrollmechanismus hinzugefügt werden, um das Risiko einzuschätzen, das mit Blick auf nicht implementierte oder korrekt umgesetzte Policies besteht. Gibt Auditoren Governance Dashboards sowie die Möglichkeit an die Hand, über den Status der verschiedenen Policies zu berichten. Außerdem Möglichkeit zur kontinuierlichen Beurteilung zentraler Kontrollmechanismen, Business-Regeln, Datenintegrität und Leistung, um sicherzustellen, dass jedes Policy-Objekt in seinem Verlauf dokumentiert und korrekt archiviert wird.

Einführung effektiver SoD-Audits
Der Lebenszyklus von Berechtigungen und Rollen kann sehr dynamisch sein. Infolgedessen können Regeln im Zusammenhang mit der Funktionstrennung (SoD) hochgradig komplex und schwer zu managen sein. Dies kann dazu führen, dass Regelwerke veralten/nicht aktuell sind und so mit Blick auf die Anwendung von Policies auch falsche Ergebnisse widerspiegeln. Ohne einen business-orientierten Ansatz kann die Organisation nur mit Mühe effektive SoD-Audits realisieren. Daher wird empfohlen, Policies zur Funktionstrennung (SoD) auf Basis von Geschäftsprozessen zu definieren, die den Standardansatz für Rollen und Genehmigungen unterstützt.

Die Liste der Geschäftsprozesse kann hierarchisch sein, wodurch es der Organisation möglich wird, sowohl feingranulare SoD als auch breitere operative Einschränkungen abzubilden. Die Organisation kann schnell neue SoD-Einschränkungen einführen, ohne ihren Rollenkatalog neu schreiben zu müssen, weil die SoD-Policy auf einem Geschäftsprozess beruht, der sich wesentlich seltener ändert.

Sicherstellen kontinuierlicher Compliance
Manche Organisationen implementieren ein- bis zweimal jährlich geplante Sicherheitsbewertungen – dieser Ansatz führt potenziell zu Sicherheitsvorfällen, die monatelang unentdeckt bleiben. In regulierten Branchen und bei missionskritischen Systemen wird dringend eine höhere Audit-Häufigkeit empfohlen. Zum konstanten Monitoring und Alarm-Auslösen bei Verstößen gegen Regeln oder Sicherheit lassen sich Policy-Auditing-Prozesse als kontinuierliche Prozesse einsetzen, mit denen Folgendes erreicht wird:

- Einrichtung konstanter Zugriffskontrollen auf geschäftskritische Daten und geistiges Eigentum.
- Erkennen und Lösen von SoD-Problemen.
- Sicherstellen, dass alle relevanten Zugriffsrechte identifizierbar sind.
- Quartalsweise Überprüfung von Regeln auf Effektivität.
- Verfeinern und Anwenden granularer Reporting- und Analysevorgänge.

Im Themenbereich Audit zu erwägende Fragen:

- Verfügen wir über ein Business Alignment?
- Wer sind die designierten Policy-Eigentümer?
- In welchen zeitlichen Abständen sollten Auditing-Prozesse durchgeführt werden?
- Mit welcher Häufigkeit sollten Policy-Reviews erfolgen?

Zusammenfassung

Hoch entwickelte Auditing-Funktionen unterstützen Business-Policies und sollten in die IGA-Prozesse von Organisationen aufgenommen werden. Ein Ausbau des IGA-Frameworks mit automatisierten Auditing-Prozessen sichert Datenintegrität durch Erkennen und Lösen von Ausnahmen, wodurch die angestrebten Policy-Ergebnisse erreicht werden. Die Nutzung von detailliertem Reporting, Analyse und Evaluierung von Policies für Identitäten, Konten, Berechtigungen, Funktionstrennung (SoD) und privilegierten Konten sorgt für ein effektives Auditing. Automatisierte Audit-Prozesse ermöglichen Vergleichsmöglichkeiten zwischen dem Ist-Zustand von Identitäten und Zugriffsrechten mit dem erwarteten bzw. Soll-Zustand, der Fähigkeit, Policy-Eigentümer auf Verstöße und Ausnahmen hinzuweisen sowie einen Workflow zur Verfügung zu stellen, der eine zügige und geordnete Problembehebung unterstützt.

Der nächste Schritt

EIN KONTINUIERLICHER PROZESS

Die verschiedenen Bereiche, die die Prozesse des IdentityPROCESS+ Framework abdecken, ermöglichen Organisationen im Laufe eines IGA-Projekts die Implementierung zahlreicher verschiedener Funktionen. Allerdings wissen Organisationen aufgrund der großen Zahl und Vielfalt von Prozessen anfangs vielleicht nicht genau, wo sie ansetzen sollen – auch wenn bei ihnen bereits eine Lösung für Identity und Access Management (IAM) implementiert ist. In diesem Abschnitt wird eine empfohlene Vorgehensweise beschrieben, um Organisationen einen Ansatzpunkt zu liefern, von dem aus sie schnell starten und den unternehmerischen Wert der Maßnahme nachweisen können.

Hierbei ist zu bedenken, dass eine IGA-Implementierung nicht nur in eine Richtung geht, sondern es in Organisationen viele verschiedene Wege gibt – je nachdem, ob die zentralen Ziele eher an Sicherheit, Compliance oder Effizienz ausgerichtet sind. Unabhängig vom eingeschlagenen Weg sind Organisationen der Auffassung, dass IGA-Implementierungen eine kontinuierliche Aufgabe darstellen, da die geschäftlichen Abläufe, die sie unterstützen, sich konstant ändern, weil neue Benutzer hinzukommen, neue Anwendungen eingeführt werden, Fusionen und Übernahmen stattfinden und zahlreiche andere geschäftliche Änderungen kontinuierlichen Support erfordern.

WIE BEGINNE ICH?

Ziele festlegen

Beim Start eines IGA-Projekts sollte man die zentralen geschäftlichen Ziele festlegen anstatt sich auf rein technische Ziele zu beschränken.

Die meisten Organisationen definieren Ziele in der Regel in folgenden Bereichen:

- Steigerung der Sicherheitslevels für Anwendungen on-premises und in der Cloud
- Verbesserung der Compliance in Verbindung mit internen Verfahren und externen Bestimmungen
- Steigerung der Effizienz durch Erhöhung der Zahl verwaltbarer Identitäten ohne Einstellen zusätzlicher Mitarbeiter in der IT-Organisation

Nach Bestimmung der allgemeinen Ziele müssen Organisationen untergeordnete Ziele festlegen, an denen sich der Projekterfolg ablesen lässt.

Beispiele für untergeordnete Ziele:

- Terminierung aller verwaisten Konten in der Organisation
- Automatisierung der Prozesse rund um das Onboarding neuer Mitarbeiter und Sicherstellung der Tatsache, dass diese ab dem ersten Arbeitstag Zugriff auf alles Erforderliche haben
- Regelmäßige Erstellung einer Reihe von Auditberichten zur Sicherstellung der Wahrung von Compliance
- Fähigkeit zur Bearbeitung sämtlicher Berechtigungsanträge von Benutzern innerhalb eines bestimmten Zeitrahmens
- Fähigkeit zur Berichterstattung über die Gründe für sämtliche Verstöße gegen Policies wie z. B. die Funktionstrennung

Einbeziehen von Stakeholdern

Nach Definition der über- und untergeordneten Ziele kann das IGA-Team die relevanten Stakeholder dazu einladen, zu diskutieren, ob die Ziele realistisch sind oder noch andere Faktoren berücksichtigt werden müssen. Da IGA-Projekte in der Regel im Grunde genommen die gesamte Organisation betreffen, ist es wichtig, sicherzustellen, dass auch Stakeholder repräsentiert sind. Auf jeden Fall anwesend sein sollten Vertreter aus den Bereichen Unternehmenssicherheit, Compliance, Auditing, IT sowie Führungskräfte, die verstehen, wie Anwendungen im Unternehmen eingesetzt werden. Um den Erfolg des IGA-Projekts sicherzustellen, ist es sehr wichtig, diese Stakeholder auf dem neuesten Stand zum Fortschritt des Projektes zu halten, um einen konstanten Buy-in zu gewährleisten.

Erstimplementierung und Quick Wins

Nach Festlegung der Projektziele und Herstellen des Kontakts zwischen mehreren Stakeholdern kann mit der eigentlichen Implementierung des IGA-Systems

begonnen werden. Wichtig ist, dem Unternehmen gegenüber einige Quick Wins vorweisen zu können, damit für die verbleibende Projektlaufzeit weiterhin wichtige Ressourcen bereitgestellt werden.

DEN WERT VON IGA-PROJEKTEN SCHON FRÜH NACHWEISEN

Importieren von HR- und Active Directory-Daten
Wie in den Prozessen von IdentityPROCESS+ beschrieben, benötigt eine IGA-Lösung Informationen aus HR-Systemen um Aufgaben wie z. B. die Zuweisung von Zugriffsrechten auf Basis von Rollen durchführen und Zugriffsanträge an die zuständigen Vorgesetzten weiterleiten zu können. Demnach ist die erste durchzuführende Aufgabe das Importieren persönlicher Angaben aus Quellsystemen – i.d.R. dem HR-System sowie allen Datenbanken für die Verwaltung von Externen – in das IGA-System. Um diese Aufgabe effektiv durchzuführen, dürfen nur qualitätsgesicherte Daten importiert werden, was bedeutet, dass Organisationen sicherstellen sollten, dass die im HR-System enthaltenen Daten vor dem Import bereinigt werden.

Nachdem Personaldaten in das IGA-System geladen wurden, ist der nächste logische Schritt das Onboarding und Importieren von Daten aus Active Directory (AD). Dies liefert dem IGA-System zusätzliche Informationen über Benutzer und ist der erste Schritt zur Kontrolle über die eigenen Daten.

Kontrolle über AD-Konten schaffen
Der erste Quick Win lässt sich schon in frühen Phasen einer IGA-Implementierung generieren, um der Organisation die Kontrolle von AD-Konten zu ermöglichen. Durch Abgleich der aus Quellsystemen importierten Daten über aktuelle Mitarbeiter und Externe mit den de facto in AD vorhandenen Accounts stellt ein Administrator rasch fest, welche AD-Konten in der Organisation keinen Eigentümer haben. Der Vergleich kann durch automatisiertes, integriertes Rule-Matching erfolgen, welches die Diskrepanzen zwischen Datenbanken zu Tage fördert. Anhand dieser Informationen kann ein Administrator feststellen, ob die Konten einem neuen Eigentümer zuzuweisen oder zu deaktivieren sind.
Diese Vorgehensweise gilt für Konten von Endbenutzern und technische Konten. Hat die Organisation diesen Prozess durchlaufen, können Administratoren zuversichtlich sein, dass keine verwaisten Konten (d.h. Konten ohne Eigentümer in AD) mehr vorhanden sind. Somit können sie garantieren, dass sämtliche Konten die AD Compliance-Anforderungen erfüllen, da sie validiert sind und über einen Eigentümer verfügen.

Durch Hinzufügen weiterer Prozesse Governance bewahren
Hat eine Organisation ein gewisses Sicherheitsniveauerlangt, gilt es, bestimmte Prozesse umzusetzen, damit dieser Zustand gewahrt bleibt. Diese nachstehend aufgeführten Prozesse sind alle im Rahmen von IdentityPROCESS+ abgedeckt.

Die drei Governance-Prozesse (Erstellen, Verwalten und Reagieren auf Rezertifizierungs-Kampagnen) schaffen konstante Compliance für Unternehmen, indem sie Manager und Ressourcen-Eigentümer anhalten, zu prüfen, ob die tatsächlichen Zugriffsrechte, die Benutzer von Anwendungen besitzen, noch gültig sind bzw. ggf. erforderliche Anpassungen vorzunehmen sind.

Der „Onboard Identity"-Prozess stellt sicher, dass neue Mitarbeiter am ersten Arbeitstag mit den benötigten Berechtigungen ausgestattet sind. Der „Onboard Contractor"-Prozess ermöglicht das Hinzufügen eines neuen Externen. Ein System-Eigentümer kann außerdem eine technische Identität über den Prozess „Request Technical Identity" erzeugen.
Die „Request Access"- und „Approval of Access Requests"-Prozesse stellen sicher, dass Benutzer nur Zugriff auf die Systeme erhalten, die sie benötigen, um ihre Aufgaben zu erfüllen. Somit behält eine Organisation die Kontrolle über die Frage, wer warum auf was Zugriff hat.

Ein weiteres zentrales Element der Wahrung der Governance ist das Managen von Mitarbeitern bei Abteilungswechseln oder Beförderungen. Die Implementierung des organisationsinternen Transferprozesses stellt sicher, dass Mitarbeitern alle zusätzlich erforderlichen Zugriffsrechte gewährt werden, ihnen gleichzeitig aber auch alle Zugriffsrechte entzogen werden, die sie nicht benötigen, damit sie nicht im Laufe der Zeit unnötige Zugriffsrechte anhäufen.
Beenden Mitarbeiter oder Externe die Zusammenarbeit mit dem Unternehmen, automatisiert der Terminierungsprozess den Entzug von Zugriffsrechten von sämtlichen Systemen, auf die die Betreffenden Zugriff haben. Ehemalige Mitarbeiter haben dadurch keinen Zugriff mehr auf Anwendungen.

Hinzufügen von Anwendungen und geschäftskritischen Systemen

So, wie man sein AD in den Griff bekommen möchte, will man alle geschäftskritischen Anwendungen unter Kontrolle bekommen. Hierzu muss zunächst die Anwendung über den „Create Target System Resource"-Prozess hinzugefügt werden. Dann wird anhand einer Berechtigungs-Zuweisungsprüfung für Manager bzw. Ressourcen-Eigentümer geprüft, ob die Zugriffsrechte des Benutzers für die Anwendungen korrekt sind. Stellt ein Manager oder Ressourcen-Eigentümer fest, dass ein Benutzer keinen Zugriff mehr haben dürfte, kann dieser widerrufen werden. Wenn die Prozesse unter Kontrolle sind, werden die gleichen Prozesse, mit denen z.B, auch die AD-Umgebung gesteuert wird, zum Management von BenutzerZugriffsrechten (Join, Move, Leave) verwendet.

WIE GEHT ES WEITER?

Hat die Organisation diese Kernprozesse implementiert, um Kontrolle zu erlangen und zu erhalten, kann ihr IGA-Projekt verschiedenste Wege gehen, um auf der geschaffenen Basis aufzubauen und so für das Unternehmen Mehrwert zu generieren.

Einige Beispiele:

- Ausweitung der Verwendung von Zuweisungs-Regeln zur weiteren Senkung von manuellem Arbeitsaufwand.
- Ausbau des als Vorlage dienenden Modells und Verwendung von Kontexten zur Senkung von administrativem Aufwand sowie Schaffung einer besseren Experience für die Organisation.
- Einführung von B2B-Identity und Access-Governance, was es B2B-Geschäftspartnern ermöglicht, auf die erforderlichen Ressourcen zuzugreifen und dennoch die Kontrolle zu behalten.
- Ausbau von Ausschlussregeln wie z. B. SoD-Policies zur Verbesserung von Compliance und Sicherheit.
- Automatisierung des Notfallsperre-Prozesses.
- Ausbau von Rezertifizierungskampagnen, um über Zugriffsdaten hinaus noch weitere Kontrolle zu schaffen.
- Einführung von Datenklassifizierung zur Verbesserung der Governance sensibler Daten.

Die Implementierung jedes dieser zusätzlichen Prozesse steigert den Return On Investment des IGA-Projekts. Es wird empfohlen, dass Organisationen in Absprache mit ihren IGA-Lieferanten an der Erstellung und Umsetzung einer Roadmap arbeiten, die sie dabei unterstützt, ihre geschäftlichen Anforderungen abzugleichen und den Wert der Organisation zu maximieren.

Glossar

Abstimmung
Prozess, bei dem bestätigt wird, dass alle gemanagten Zielsystemkonten und Zugriffsrechte die vorhandenen Vorgaben erfüllen. So müssen z. B. der Soll-Zustand aller Konten in allen gemanagten Systemen und ihre Zugriffsrechte dem Ist-Zustand Zugriff entsprechen. Die Abstimmung sollte regelmäßig erfolgen, um alle evtl. Diskrepanzen zwischen Ist- und Soll-Zustand zu beseitigen.

Access Management
Der Prozessbereich IdentityPROCESS+ zum Managen der Zugriffsrechte für neue Mitarbeiter oder bei Wechsel der Tätigkeit innerhalb der Organisation.

Actual State (Ist-Zustand)
Die Zugriffsrechte, die ein Benutzer momentan auf eine Fachanwendung hat. Die betreffenden Informationen werden von den Anwendungen eingelesen und zur Feststellung der Compliance herangezogen. Hierzu erfolgt ein Abgleich mit dem Soll-Zustand.

Administration
Der Prozessbereich IdentityPROCESS+, der die Integration von Zielsystemen in das IGA-System managt, um sowohl zentrale Administration von Benutzerzugriff und Governance als auch Password-Management zu ermöglichen.

Berechtigungsantrag
Ein Prozess, bei dem Endbenutzer ihre Vorgesetzten oder Ressourcen-Eigentümer bitten, ihnen Zugriff auf eine Fachanwendung zu geben.

Business alignment
Der Prozessbereich von IdentityPROCESS+, der IGA-Prozesse für nicht-technische Benutzer und somit auch die Verwaltung von Zugriffsrechten für Mitarbeiter mit identischer Position vereinfacht – oder für Mitarbeiter, die im selben Geschäftsbereich oder am gleichen Projekt arbeiten.

Daten-Administrator
Ein Mitglied der IT-Abteilung, das für Planung, Organisation und Kontrolle von Datenressourcen in der Organisation zuständig ist.

Datenklassifizierung
Prozess, bei dem Daten-Administratoren und Ressourcen-Eigentümer die Daten, für die sie zuständig sind, nach Typen klassifizieren. Diese Klassifizierungen werden dann zur Umsetzung von Policies verwendet, um sicherzustellen, dass die Datenverarbeitung bestimmten Vorgaben entspricht.

Direktzuweisungen
Verwendet eine Identität den Standard-Zugriffsantrags-Prozess und hat sie die Genehmigung für eine Berechtigungs-Zuweisung erhalten, wird eine mit den Identitäten verbundene Berechtigungs-Zuweisung erstellt.

Einschränkungsregel
Eine Regel, die verhindert, dass Endbenutzer Zugriff zu verschiedenen Systemen erhalten – was sie aufgrund der ihnen gewährten Zugriffslevels zur Durchführung betrügerischer Handlungen befähigen könne. Bei Verstößen gegen Ausschlussregeln sollte der im Unternehmen verfügbare Zugriff auf verschiedene Mitarbeiter aufgeteilt werden, um das Risiko schädlicher Aktivitäten zu senken. Siehe auch „Funktionstrennung".

Fachanwendung
Eine Anwendung innerhalb der Organisation, für die Benutzer Zugriff benötigen, damit sie ihre Aufgaben wahrnehmen können. Mögliche Beispiele: ein CRM-System, E-Mail oder eine Produktionsdatenbank.

Funktionstrennung (SoD)
Ein Prinzip, das die Trennung zwischen Organisationseinheiten oder Stellen im Geschäftsprozess zur Vermeidung von möglichen Interessenkonflikten sicherstellt. IdentityPROCESS+ definiert einen Prozess zur Erkennung der Zuordnung beliebiger riskanter Zugriffskombinationen und verhindert die Gewährung solcher Zugriffsrechte ohne Angabe bestimmter Gründe und Genehmigung durch Sicherheitsbeauftragte.

HR-System
Das HR-System liefert in der Regel die aktuellsten und präzisesten Informationen über den Anstellungsstatus der Belegschaft und wird daher bei IGA-Implementierungen als Quellsystem verwendet.

Identity Lifecycle Management
Der Prozessbereich IdentityPROCESS+ zum Managen der Berechtigungen über die gesamte Beschäftigungszeit einer Person – vom Eintritt ins Unternehmen über die gesamte Anstellungszeit bis zur Beendigung der Zusammenarbeit.

Identität
Darstellung einer physischen Person oder technischen Identität durch ein eindeutig definiertes Objekt mit einer bestimmten, diesem zugeordneten Informationsmenge; der Zugriff der Identität auf Systeme ist zu dokumentieren und managen.

Klassifikationskennzeichen
Eine Methode, mit der System-Eigentümer die in ihren Datenanwendungen vorhandenen Datentypen identifizieren können, um geeignete Policies zur Einhaltung interner Regeln und externer Bestimmungen wie z. B. DSGVO anwenden zu können.

Kontext
Methode zur Gruppierung von Benutzern in Organisationseinheiten, damit diese in gleicher Weise gemanagt werden können. Ein Kontext könnte z. B. eine Gruppe von Personen sein, die am gleichen Projekt arbeiten, dieselbe Kostenstelle teilen oder im gleichen Werk tätig sind.

Konto
Ein Benutzer- oder technisches Konto in einem System –beispielsweise einem Active Directory-Konto –, dem Zugriff zu Ressourcen (Zugriffsrechte) in einem System zugewiesen oder gewährt werden.

Notfallsperre
Die schnelle Deaktivierung aller mit einer Identität verbundenen Konten bei Verdacht auf einen Sicherheitsvorfall. Soll Angreifer davon abhalten, weiterhin auf die Daten eines Unternehmens zuzugreifen bzw. Anwendungen in ihrer Funktion zu stören.

Offboarding
Der Prozess des Sicherstellens, dass Mitarbeiter, Externe und andere Benutzer nach Beendigung ihrer Zusammenarbeit mit einer Organisation nicht mehr auf deren Anwendungen zugreifen können.

Onboarding
Der Prozess des Sicherstellens, dass Mitarbeiter, Externe und andere Benutzer bei Beginn ihrer Zusammenarbeit mit dem Unternehmen geeigneten Zugriff zu Anwendungen erhalten, um ihre Aufgaben durchzuführen.

Policy/ Regel
Eine Policy legt fest, dass eine Reihe von Identitäten Zugriff zu einer Reihe von Rollen/ Ressourcen haben sollten (Zuweisungs-Regel) oder von der Zuweisung bestimmter Kombinationen aus Regeln/Ressourcen ausgeschlossen sein sollten (Ausschlussregel). Policies sind Definitionen erlaubter bzw. verbotener Kombinationen von Identitäten, Rollen und Kontexten.

Prozess
Die Beschreibung einer Reihe von Maßnahmen, die in einem IGA-System durchgeführt werden können.

Prozessbereich
IdentityPROCESS+ definiert sieben Prozessbereiche: Identity Lifecycle Management, Access Management, Business Alignment, Identity Security Breach, Governance, Administration und Auditing.

Provisionierung
Die systemübergreifenden Prozesse zur Erstellung, Änderung und Deaktivierung von Konten und Privilegien. Die Provisionierung kann entweder manuell oder automatisch durch technische Integration vorgenommen werden.

Process group
A collection of IGA processes whose tasks are related and therefore are logically grouped and implemented together.

Quellsystem
Die Hauptquelle für Personaldaten; wird vom IGA-System zur Umsetzung von Regeln und Prozessen verwendet. In den meisten Organisationen ist das Quellsystem das HR-System, da sich dort die aktuellsten Daten über Mitarbeiter befinden, die in das Unternehmen eintreten bzw. es wieder verlassen; sowie außerdem Angaben über deren aktuellen Jobtitel und Vorgesetzten.

Ressource
Eine Berechtigung oder eine Gruppe von Berechtigungen, die in einem physischen System durch das Access-Control-Modell dieses Systems definiert sind. Gruppen in einem Directory Service wie z. B. Active Directory gelten als Ressourcen.

Ressourcen-Eigentümer
Für das Management einer Ressource verantwortlicher Administrator.

Rezertifizierung
Die regelmäßige oder spontane Überprüfung und Validierung der Korrektheit und Gültigkeit von Zugriffsrechten, Policies, Rollendefinitionen und Stammdaten im System. Die häufigsten Rezertifizierungskampagnen überprüfen den Zugriff von Identitäten auf Ressourcen in Zielsystemen.

Rezertifizierungskampagne
Eine Umfrage, die an Vorgesetzte und Ressourcen-Eigentümer verschickt wird, um im IGA-System gespeicherte Informationen wie z. B. Zugriffsrechte, Policies, Rollendefinitionen und Stammdaten zu überprüfen.

Rolle
Sammlung von Ressourcen aus einem oder mehreren Systemen oder anderen Rollen. Rollen können Identitäten zugewiesen werden (z. B. „diese Person hat diese Rolle“).

Sicherheitsvorfälle
Der Prozessbereich von IdentityPROCESS+, der eine Notfallsperrung und die Wiederherstellung von Zugriff auf Benutzerkonten veranlasst, wenn eine Organisation den Verdacht hat, dass ein Sicherheitsverstoß begangen wurde.

Soll-Zustand
Sicherstellung, dass die Zugriffsrechte, über die Benutzer idealerweise verfügen sollten, den Compliance- und Sicherheits-Standards entsprechen. Diese Informationen werden mit dem Ist-Zustand verglichen, um festzustellen, ob es Verstöße beim Benutzerzugriff gab, gegen die dann der Administrator tätig werden muss.

Stammdaten
Persönliche Informationen über einen Mitarbeiter oder Externen wie z. B. Name, Jobtitel sowie Vorgesetzter; werden aus einem oder mehreren Systemen (in der Regel dem Quellsystem) zusammengestellt, in einem zentralen Datenspeicher abgelegt und vom IGA-System für Aufgaben wie z. B. der Durchsetzung von Policies und der Weiterleitung von Zugriffsanträgen herangezogen.

System
Ein technisches System wie z. B. Active Directory, eine Finanzanwendung oder ein HR-System.

System-Eigentümer
Für das Management eines Systems verantwortlicher Administrator.

Technische Identität
Eine Identität, die verwendet wird, um mehreren Mitgliedern des IT-Teams Administratorenzugriff zu Systemen zu verschaffen, ohne dass diese hierfür ihre persönliche Identität heranziehen müssen. Da diese Identitäten über privilegierte Zugriffsrechte verfügen und von mehreren Mitarbeitern verwendet werden, müssen sie sorgfältig gehandhabt werden, um Missbrauch zu vermeiden.

Umfrage/ Kampagne
Eine Umfrage besteht aus einer Reihe von Fragen, die an Vorgesetzte und Ressourcen-Eigentümer verschickt werden und bei denen die Befragten um Attestierung bzw. Rezertifizierung ihrer Benutzer-Zugriffsrechte ersucht werden.

Verwaistes Konto
Einem Konto ist keine Person zugeordnet. Dies kann daher kommen, dass der Mitarbeiter das Unternehmen verlassen hat, sein Konto aber nicht deaktiviert wurde; oder es wurde unterlassen, eine technische Identität einem Eigentümer zuzuordnen. Verwaiste Konten sollten entweder einem Eigentümer zugewiesen oder deaktiviert werden, da sie ansonsten nicht ordentlich verwaltet werden können.

Zielsystem
Eine ins IGA-System integrierte Fachanwendung, durch die Benutzer-Zugriffsrechte zentral gemanagt werden können.

Seit dem Jahr 2000 arbeitet Omada fokussiert daran, Business Value durch Verwendung einer IGA-Lösung zu schaffen. Unternehmen, die ihre Identitäten mit der Omada Identity Suite verwalten, steigern gleichzeitig die Sicherheit, die Effizienz, die Kostenkontrolle und stellen die Einhaltung gesetzlicher Vorgaben in ihrer Organisation sicher. Eine professionelle Lösung zur Verwaltung von Identitäten kann den digitalen Umbau und reibungslose M&A-Integrationsprozesse beschleunigen, aber sich auch positiv auf die Beziehungen mit Lieferanten und Kunden auswirken. Nur wenige Technologien haben eine solche Reichweite. Wir haben in diesem Bereich Pionierarbeit geleistet sowie zahlreiche Best Practices entwickelt. Wir arbeiten engagiert daran, Business Value durch den Einsatz der Omada Identity Suite zu schaffen.

Omada

omadaidentity.com