Kennen Sie Ihre Benutzer?

Ein AdNovum IT Consulting Whitepaper, Oktober 2012

ADNOVUM

Über AdNovum IT Consulting

AdNovum konzipiert, implementiert und pflegt seit bald 25 Jahren anspruchsvolle Software-Lösungen für Firmen und Behörden. Das Wissen und die Erfahrung aus der Projektarbeit geben wir in Form von Beratung an unsere Kunden weiter. Sie finden bei uns hersteller- und produktunabhängige Unterstützung für komplexe IT-Vorhaben. Unser Angebot umfasst alle Lösungsebenen, von technologischen Fragen über die Prozessgestaltung bis hin zur IT-Strategie-Beratung.

Identity- und Access-Management (IAM) ist eine der Kernkompetenzen von AdNovum. AdNovum hat für eine Vielzahl namhafter Kunden aus dem öffentlichen und dem privaten Sektor IAM-Lösungen beurteilt, entworfen und implementiert. Dazu gehören die Analyse existierender Benutzeraccounts, die Konzeption von Lösungen zur Zugriffssteuerung, die Benutzer- und Rechteverwaltung sowie die Projektbegleitung.

http://www.adnovum.ch

Über die Autoren

Peter Gassmann leitet seit April 2012 das IT Consulting der AdNovum Informatik AG, bei der er seit Sommer 2010 zunächst als Senior IT Consultant und Identity Architect tätig war. Davor arbeitete er 10 Jahre für Sun Microsystems, ebenfalls im Bereich Identity-Management. Bei AdNovum berät Herr Gassmann Kunden rund um Security und Identity- und Access-Management und leitet auch Projekte in diesem Umfeld.

Thomas Zweifel, seit 2006 bei AdNovum, ist Dipl. Inf.-Ing. ETH und MAS ETH MTEC. Als Senior Software Security Engineer, technischer Projektleiter und IT Consultant hat er für AdNovum an einer Vielzahl von Projekten mitgewirkt, insbesondere in Projekten mit Fokus IT Security, Identity- und Access-Management sowie IT-Strategie. Davor war Thomas Zweifel während sechs Jahren für seine eigene Firma tätig. Heute berät und leitet er Projekte in diesen Bereichen.

Kennen Sie Ihre Benutzer?

Datendiebstahl und unerlaubte Transaktionen gehören für Unternehmen zu den bedeutendsten Risiken in der IT. Es ist essentiell zu wissen, welcher Benutzer was gemacht hat. Die Nachvollziehbarkeit muss nicht nur im Auditfall gewährleistet sein, sondern auch im Falle eines unerwünschten Ereignisses wie Datendiebstahl. Oft werden dabei Benutzeraccounts mit entsprechenden Zugriffsberechtigungen verwendet. Im Kontext von Governance, Risk und Compliance (GRC) empfiehlt sich daher eine systematische Kontrolle der Benutzerkonten und -berechtigungen. Im Folgenden werden Einflussfaktoren, Risiken und Lösungsansätze rund um Benutzeraccounts erklärt und aufgezeigt.

Für Applikationen im geschäftlichen Umfeld benötigt man normalerweise einen persönlichen Benutzeraccount, welcher die Identität eines Benutzers in der Applikation repräsentiert. Der persönliche Benutzeraccount erlaubt die Zuordnung von Berechtigungen zur Identität zum Zweck der Steuerung sowie zum Zweck der Nachvollziehbarkeit. Die Berechtigungen definieren, welche Aktionen ein Benutzer in der Applikation ausführen darf. Wenn sich ein Benutzer nun mit seinem Account in die Applikation einloggt, weiss diese, welcher Benutzer angemeldet ist, und kann dadurch für jede Aktion überprüfen, ob der Benutzer dafür berechtigt ist. Ebenso kann für jede ausgeführte Aktion festgehalten und auditiert werden, welcher Benutzer sie unter welchen Umständen vorgenommen hat.

Einflussfaktoren auf Benutzeraccounts

Benutzeraccounts unterstehen wie in *Abbildung 1* visualisiert einer Vielzahl von Einflussfaktoren, welche zum grossen Teil direkt durch das Unternehmen beeinflusst werden können, das die geschäftlichen Applikationen kontrolliert.

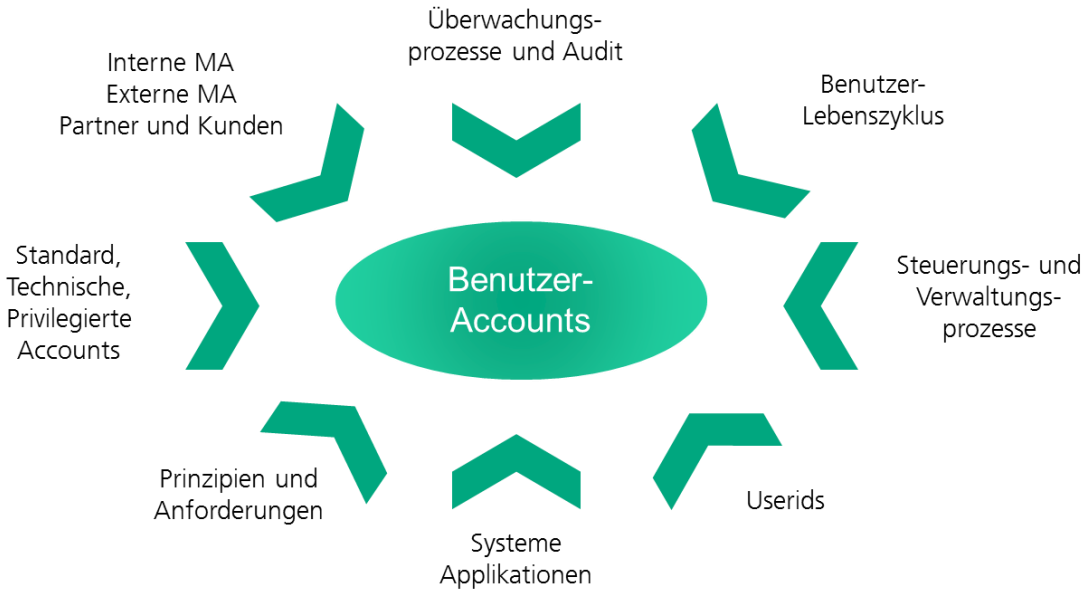

Abbildung 1: Einflussfaktoren auf Benutzeraccounts

Diese Einflussfaktoren werden in den folgenden Abschnitten erläutert. Ein Teil dieser Faktoren, z.B. die Steuerungs- und Verwaltungsprozesse, können durch das Unternehmen definiert und gesteuert werden. Für diejenigen Faktoren, die nicht direkt beeinflusst werden können, müssen Wege gefunden werden, um allfällige Risiken zu erkennen und eine zuverlässige Kontrolle und Nachvollziehbarkeit zu ermöglichen.

Prozesse rund um Benutzeraccounts

Benutzeraccounts unterliegen einem Lebenszyklus, der die Erzeugung, Modifikation, Aktivierung, Deaktivierung und schlussendlich Löschung oder Archivierung des Accounts umfasst. Benutzeraccounts werden innerhalb ihres Lebenszyklus von einer Vielzahl von Ereignissen beeinflusst. So werden z.B. dem für den Account zuständigen Mitarbeiter je nach Funktion und Aufgabe Berechtigungen zugeordnet oder entzogen. Ein möglicher Lebenszyklus eines internen Mitarbeiters ist in *Abbildung 2* wiedergegeben.

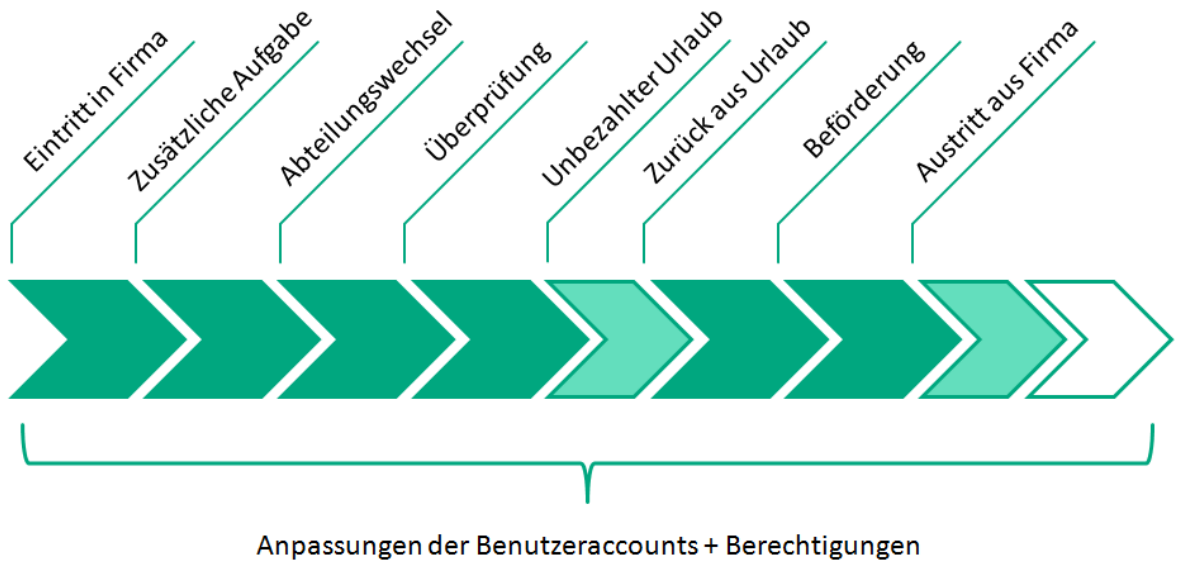

Abbildung 2 Benutzerlebenszyklus eines internen Mitarbeiters

Für die regulären Mitarbeiter sind die Personalverwaltungsprozesse eng mit dem Lebenszyklus der jeweiligen Benutzeraccounts innerhalb der Firma gekoppelt. Startpunkt ist der Eintritt in die Firma, dann kann es Mutationen, Beförderungen, Reorganisationen und andere Veränderungen geben. Am Schluss steht der Austritt aus der Firma. Diese an Personalprozesse angelehnten Berechtigungsprozesse sind bei den meisten Unternehmen wohldefiniert und eingespielt. Bei nicht persönlichen Accounts sind solche Abläufe jedoch selten klar geregelt und überwacht, unabhängig davon ob es sich um privilegierte Accounts, technische Accounts oder Test- und Schulungs-Accounts handelt.

Auch für externe Personen ist der Lebenszyklus nicht immer klar definiert. Oft wird zwar festgelegt, wie ein Benutzer angelegt oder importiert werden kann, jedoch nicht, wie regelmässige Überprüfungen durchgeführt werden oder wer den Benutzer sperrt, falls er aus der Drittfirma austritt und dadurch der externe Account gesperrt oder gelöscht werden müsste. In diesem Zusammenhang ist nicht immer klar, welche Datenquellen für externe Benutzer verwendet werden können und wie diese gepflegt werden. So beinhaltet ein Customer Relationship Management-Tool (CRM-Tool) unter Umständen mehr Angaben zu Partnern und Kunden als das Identity Management-Tool. In diesem Bereich ist die Aktualität und Qualität der verfügbaren Daten oft ungenügend.

Die Benutzerverwaltungs- und Berechtigungsprozesse müssen alle Applikationen einbeziehen, in denen Benutzeraccounts oder Berechtigungen benötigt werden. Je mehr Applikationen eine eigene Benutzerverwaltung beinhalten, desto aufwändiger werden folglich die Umsetzung der Prozesse sowie die Sicherstellung der Konsistenz zwischen Soll-Zustand und Ist-Zustand.

Fehlende Berechtigungen – Kein Problem …?

Normalerweise hat der Mitarbeiter ein direktes Interesse daran, die Berechtigungen zu erhalten, die er zur Ausführung einer Aufgabe braucht. Er wird sich solange aktiv um diese Berechtigungen bemühen, bis er sie hat. In vielen Firmen funktioniert dieser Prozess sehr gut, weil er ein Stück weit reaktiv und passiv gestaltet werden kann: Der Benutzer beantragt eine Berechtigung, der Antrag wird validiert, die Berechtigung wird vergeben. Falls etwas schief läuft, wird sich der Benutzer melden.

Wird sich aber ein Benutzer melden, wenn er zu viele Berechtigungen hat? Oder wenn er einen Zugriff auf ein System nicht mehr benötigt? Kaum. Denn für den Benutzer stellt dies kein Problem dar. Er kann seine Aufgaben trotz zu vieler Berechtigungen wahrnehmen. Ausserdem müsste der Benutzer selber überhaupt erst erkennen, dass er zu viele Berechtigungen hat. Ein gutes Illustrationsbeispiel für zu viele Berechtigungen sind Auszubildende: In vielen Firmen arbeiten sie nacheinander in verschiedenen Abteilungen, um einen Gesamtüberblick über die Arbeitsprozesse und Bereiche der Firma zu erhalten. Da sie die Berechtigungen der jeweils aktuellen Abteilung benötigen, um produktiv tätig zu sein, akkumulieren sie nach und nach sämtliche Berechtigungen, die ein Mitarbeiter in der Firma haben kann, obwohl sie diese eigentlich gar nicht mehr benötigen, nachdem sie eine Abteilung wieder verlassen haben. Interne Wechsel sind daher grundsätzlich als Anlass für eine Überprüfung und Bereinigung der Berechtigungen zu nehmen.

Zu viele Berechtigungen – Risiken und Kosten

Wenn Mitarbeiter zu viele Berechtigungen haben, kann das dazu führen, dass sie definierte Prozesse umgehen. So könnte zum Beispiel jemand seine eigenen Bestellungen autorisieren, obwohl dies nicht vorgesehen ist. Tatsächlich sind einige der bekanntesten Betrugsfälle der letzten Jahre – speziell im Bankenumfeld – darauf zurückzuführen, dass ein Mitarbeiter zu viele Berechtigungen hatte oder sich diese verschaffen und so die Kontrollen aushebeln konnte. Ein besonders hohes Risiko besteht bei Mitarbeitern, die mehrere Benutzeraccounts kontrollieren oder sich mit einem technischen Account anmelden können. Viele Firmen tun sich noch immer schwer damit, zu viele Berechtigungen überhaupt zu erkennen. Nur schon die Zuordnung aller Accounts zum jeweiligen Mitarbeiter ist nicht immer eindeutig. Dazu kommen Berechtigungen, die nur technisch beschrieben sind und dem geschäftlichen Kontext nicht eindeutig zugeordnet werden können.

Neben dem Risiko von Betrugsfällen existiert aber auch das Risiko der beabsichtigten oder unbeabsichtigten Zerstörung von Daten. Privilegierte Accounts werden oft für die Ausführung von Massenoperationen verwendet, und dies zum Teil ohne Einschränkung auf allen Daten im System. Da Fehlmanipulationen in der täglichen Arbeit hin und wieder vorkommen, steigt mit einem solchen Account das Risiko, dass eine grosse Menge an Daten von einem Fehler betroffen ist. Auch die unsachgemässe oder unbefugte Verwendung von technischen Accounts stellt ein erhebliches Risiko dar, da solche Accounts oft umfangreiche Berechtigungen haben, zum Beispiel für Synchronisationszwecke.

Besondere Aufmerksamkeit ist jenen Benutzern zu schenken, die über eine Berechtigung für einen Remote-Zugang zur Firmen-Infrastruktur verfügen. Dazu gehören auch externe Dienstleister, bei denen manchmal Zugangsinformationen von mehreren Benutzern geteilt werden, zum Beispiel für Remote Support.

Nicht zuletzt können überflüssige Berechtigungen auch direkt Mehrkosten verursachen: Applikationen werden teilweise nach der Anzahl registrierter Benutzer lizenziert. Folglich generiert jeder Benutzeraccount, der eigentlich nicht (mehr) gebraucht wird, unnötige Kosten. Durch eine aktive Nachverfolgung der Nutzung und eine zeitnahe Deaktivierung von ungenutzten Zugängen können hier ebenfalls Kosten eingespart werden.

Nachvollziehbarkeit gewährleisten

Neben der Steuerung der Applikationen durch die gezielte Zuweisung von Berechtigungen wird auch der Nachvollziehbarkeit grosse Bedeutung beigemessen. Wenn einmal etwas schief gelaufen ist, sollte es zumindest möglich sein, über Audit-Logs nachzuvollziehen, wer welche Aktionen wann gemacht hat. In diesem Fall stellt die Benutzer-ID des verwendeten Accounts die Verbindung zum Mitarbeiter dar, der allenfalls zur Rechenschaft gezogen werden soll.

Unterschiedlichste Account-Typen

In einer einzelnen Applikation können unterschiedliche Arten von Benutzeraccounts benötigt werden. Die Account-Typen unterscheiden sich nach Benutzerkreis und Einsatzzweck. Je nachdem ergeben sich daraus unterschiedliche Risikoprofile wie auch unterschiedliche Prozesse. Die Risikoprofile geben einen Hinweis darauf, wie gross das Risiko für den Betreiber der Applikation ist, wenn ein entsprechender Account auf nicht vorgesehene oder gar kriminelle Art verwendet wird. Die folgende *Tabelle 1* gibt einen Überblick über die Account-Typen.

Typ	Beschreibung	Risikoprofil
Standard-Account	Persönlicher Account für die tägliche Arbeit	Normales Risiko, sofern ein Lebenszyklus von der Erstellung bis zur Löschung des Accounts definiert ist. Sofern dies der Fall ist, sind persönliche Accounts meistens gut überwacht und damit vorgenommene Aktionen einer Person zuordenbar.
Persönlicher privilegierter Account	Persönlicher Account mit zusätzlichen oder speziellen Berechtigungen, z.B. für administrative Aufgaben.	Erhöhtes Risiko aufgrund erweiterter Rechte
Nicht persönlicher privilegierter Account	Account mit zusätzlichen oder speziellen Berechtigungen, z.B. für administrative Aufgaben.	Hohes Risiko, da der Account nicht einer Person zugeordnet werden kann. Dadurch ist die Verantwortlichkeit unklar und die Nachvollziehbarkeit nicht gewährleistet.
Technischer Account	Account, der von einer Applikation zur Interaktion mit einer anderen Applikation verwendet wird.	Erhöhtes Risiko, da der Account nicht einer Person zugeordnet werden kann und Standardpolicies wie Passwortwechsel kaum umsetzbar sind.
Schulungs-Account / Test-Account	Account, der für Schulungen oder für Tests verwendet wird. Findet sich idealerweise nur in Testsystemen.	Tiefes Risiko, sofern die Testumgebung abgetrennt ist. Erhöhtes Risiko, falls die Testumgebung mit Produktivsystemen verbunden ist, da solche Accounts meistens wiederverwendet werden und dadurch nicht persönlich sind.
Externer Account	Account einer Person, die nicht direkt bei der Firma angestellt ist. Häufig für externe Mitarbeiter, Lieferanten oder Partner.	Erhöhtes Risiko, da die Umsetzung der Lifecycleprozesse bei externen Personen anspruchsvoller und fehleranfälliger ist.
Kunden-Account	Account eines Kunden	Erhöhtes Risiko, falls Zugriffe auf firmeninterne Systeme konfiguriert sind, da die Umsetzung der Lifecycleprozesse bei Kunden anspruchsvoller und fehleranfälliger ist.

Tabelle 1: Übersicht Benutzeraccount-Typen

Einige der Account-Typen in der obigen Tabelle sind eindeutig einer Person zugeordnet. Dazu gehören Standard-Accounts, persönliche privilegierte Accounts, Accounts für Kunden und externe Mitarbeiter. Persönliche Accounts können beim Eintritt der betreffenden Person in das Bezugsfeld der Applikation sowie bei ihrem Austritt entsprechend angepasst werden, sofern die Informationen zeitnah vorliegen.

Neben den personenbezogenen Accounts gibt es technische Accounts, die von Systemen und Applikationen bei Zugriffen auf andere Systeme und Applikationen genutzt werden. Technische Accounts unterscheiden

sich aus Applikationssicht nicht von Accounts für normale Benutzer. Allerdings erfolgt ihre Nutzung nicht interaktiv, deshalb sind die Authentisierungsmittel bzw. Credentials typischerweise auf den Systemen hinterlegt. Durch die Hinterlegung auf Systemen können Schutzmechanismen wie regelmässige Passwortwechsel für diese Accounts oft nicht genutzt werden, denn die Verantwortung liegt in der Regel nicht bei einer einzelnen Person, sondern bei einem Team, wodurch die Szenarien von nicht persönlichen Accounts berücksichtigt werden müssen. Durch die Hinterlegung der Credentials in einem System entsteht zusätzlich ein Risiko durch unberechtiges Auslesen, welches einen Missbrauch dieses Accounts ermöglichen kann. Dass technische Accounts ausserdem oft in Szenarien mit erhöhten Berechtigungen eingesetzt werden, kann das Risikopotential weiter erhöhen.

Für die Schulung neuer Mitarbeiter, aber auch bei der Einführung einer neuen Applikation werden Schulungs- und Test-Accounts eingerichtet. Wo vorhanden wird dafür ein Testsystem verwendet, um allfällige Fehlbedienungen im produktiven System zu vermeiden und neue Applikationen ausführlich testen zu können. Je nach Konfiguration, Systemarchitektur und Verfügbarkeit von Testsystemen kommt es auch vor, dass solche Accounts im produktiven Umfeld erstellt und genutzt werden. Dadurch ergibt sich analog zu nicht persönlichen Accounts ein erhöhtes Risiko, da die Nachvollziehbarkeit nicht mehr gegeben ist.

Zusätzlich zu den bisher genannten Accounts gibt es auch Benutzergruppen, die nicht direkt im Einflussbereich des Unternehmens stehen, sondern externe Accounts nutzen: Dazu gehören etwa Mitarbeiter anderer Unternehmen wie zum Beispiel Lieferanten, Partner oder Firmenkunden oder Endkunden, die Zugriff auf die Infrastruktur des anbietenden Unternehmens benötigen.

Da die Zugriffe über externe Accounts oftmals unregelmässig und seltener erfolgen, ist die Umsetzung von Sicherheitsrichtlinien hier schwieriger. Auch will man Endkunden zum Beispiel nicht mit Regeln für komplexe Passwörter mit häufigem Passwortwechsel abschrecken. Ebenfalls kann es sein, dass der Einsatz von starker Authentisierung mittels Zusatzgeräten aus Kostengründen nicht in Frage kommt.

Privilegierte Accounts

Um administrative Funktionen in einer Applikation zu nutzen, sind spezielle Berechtigungen nötig. Für Administratoren werden deshalb oft sogenannte privilegierte Accounts erstellt mit der Motivation, dass diese Accounts gezielt und bewusst für Administrationstätigkeiten genutzt werden, die mit einem normalen Benutzeraccount nicht möglich sind.

Bei solchen privilegierten Accounts muss zwischen persönlichen und nicht persönlichen, potentiell von mehreren Benutzern geteilten Accounts unterschieden werden: Bei persönlichen privilegierten Accounts besteht aufgrund der zusätzlichen Privilegien ein erhöhtes Risiko, dieses kann jedoch mittels regelmässiger Überprüfung der Notwendigkeit der Privilegien sowie durch zusätzliche Schutzmechanismen wie Passwortvorgaben oder der Nutzung von starker Authentisierung wie Zertifikaten geschützt werden. Bei nicht persönlichen privilegierten Accounts wie zum Beispiel *root* auf Unix-basierten Systemen ist dies jedoch nur beschränkt möglich: Dadurch entsteht generell ein hohes Risiko, das genauer betrachtet und bewertet werden muss.

Die oben aufgeführten Account-Typen dienen dem Verständnis und der Gruppierung der unterschiedlichen Risiken, die im Umfeld von Benutzerverwaltung und Zugriffskontrolle existieren. Für eine vollständige Kontrolle und Betrachtung der Risiken rund um Benutzeraccounts ist es notwendig, all diese Account-Typen und damit die entsprechenden Benutzergruppen in die Betrachtungen einzubeziehen. Die Erarbeitung von entsprechenden Massnahmen muss die Unterschiede zwischen den Benutzergruppen berücksichtigen und auf die konkreten Bedürfnisse abgestimmt werden.

Prinzipien der Risikominimierung

Es existieren verschiedene Grundprinzipien, um Benutzeraccounts möglichst konform zu den Geschäftsprozessen und Vorschriften zu halten. Die Einhaltung dieser Prinzipien hilft, die Risiken zu minimieren.

Am wichtigsten ist das "least privilege"-Prinzip, das Prinizip der geringsten Rechte. Dieses besagt, dass ein Benutzer nur genau jene Berechtigungen haben sollte, die er für die Erfüllung seiner Aufgabe zwingend benötigt. Berechtigungen sollten also nicht nach dem Giesskannenverfahren wahllos an alle Mitarbeiter verteilt werden, sondern strikt unter Berücksichtigung der Geschäftsprozesse und der Rolle, die der Mitarbeiter aktuell darin hat. Hierzu gehört auch der Entzug von Berechtigungen, sobald diese nicht mehr benötigt werden, wie dies in obigem Beispiel für Auszubildende der Fall ist.

Ein weiteres wichtiges Prinzip, das als "segregation of duties" bezeichnet wird, ist die Trennung von Aufgaben: Wiederum basierend auf den Geschäftsprozessen ist zu definieren, welche Rollen in den Prozessen nicht durch ein und dieselbe Person übernommen werden dürfen. Damit lässt sich sicherstellen, dass eine einzelne Person nicht ohne weiteres wichtige Kontrollschritte umgehen kann. Ebenfalls im Zusammenhang mit Kontrollen steht das 4-Augen-Prinzip. Dieses verlangt, dass bestimmte Prozessschritte von mehreren Personen bestätigt werden müssen. Auch dieses Prinzip erschwert es einem einzelnen Mitarbeiter, die Prozesse auszuhebeln.

In der folgenden *Tabelle 2* sind die Prinzipien zusammengefasst:

Prinzip	Beschreibung
Least Privilege	Jeder Benutzer besitzt nur genau die Rechte, die er für seine Arbeit unbedingt benötigt.
Segregation of Duties	Sich ergänzende Pflichten müssen von unterschiedlichen Personen durchgeführt werden, um einen Missbrauch von Rechten zu erschweren.
Keep it simple	Einfache, verständliche Sicherheitsmechanismen und Konzepte reduzieren die Fehlermöglichkeiten.
Open Design	Die Sicherheit eines Systems darf nicht von der Geheimhaltung des Designs der Sicherheitsmechanismen abhängig sein – also keine Security through Obscurity.
Fail-Safe Defaults	Sämtliche Zugriffe sind grundsätzlich verboten, ausser die Berechtigung wurde explizit erteilt.
Complete Mediation	Sämtliche Zugriffe werden stets validiert, bevor sie ausgeführt werden.
Psychological Acceptability	Die Nutzung eines Systems darf durch die zusätzlichen Sicherheitsmechanismen nicht unnötig komplexer werden als bei der Verwendung ohne Sicherheitsmechanismen.

Tabelle 2: Wichtige Grundprinzipien

Diese Prinzipien gelten sowohl bei der Gestaltung der Benutzerverwaltungs- und Zugriffsprozesse wie auch beim Design und der Umsetzung von Applikationen.

Herausforderungen und Lösungsansätze

Die genannten Risiken im Zusammenhang mit falsch vergebenen Berechtigungen können durch geeignete Implementierungen der geschilderten Prinzipien adressiert werden. Die Umsetzung der Prinzipien bedingt, dass für die Geschäftsprozesse die Funktionen und Rollen und die damit verbundenen benötigten Berechtigungen in den Applikationen definiert sind. Damit kann für jeden Benutzer festgelegt werden, welche Rolle er im Rahmen der Prozesse einnimmt, wobei ein Benutzer mehrere Rollen einnehmen kann. Ohne diese Definition der applikatorischen Rollen sind Kontrollen nicht möglich. Hier stellt sich bereits die erste Herausforderung, da insbesondere bei älteren Applikationen die benötigte Dokumentation oder das Wissen dazu häufig fehlt oder aber unvollständig ist. Bei Applikationen, die schon sehr lange in Betrieb sind, kann die nachträgliche Erarbeitung der Dokumentation mit viel Aufwand verbunden sein.

Bei der Erarbeitung von Rollen als Abstraktionsschicht für Applikationsberechtigungen ist darauf zu achten, dass die Rollen intuitiv sind und allfällige technische Werte verständlich aufzeigen. Dies ist essentiell, da die Berechtigungen nicht von Informatikern, sondern von Vorgesetzten in den Fachabteilungen vergeben werden sollen, da diese die fachlichen Zusammenhänge und Bedürfnisse verstehen. Gleichzeitig ist darauf zu achten, dass das Rollenmodell nicht zu komplex wird oder gar dazu führt, dass es für die Mitarbeiter mühsam oder unmöglich wird, die für die Erledigung von geschäftsrelevanten und geschäftskritischen Prozessen notwendigen Berechtigungen rechtzeitig zu erhalten.

Des Weiteren fehlt manchmal eine zentrale Stelle, die pro Mitarbeiter eine eindeutige, für alle Applikationen gültige Benutzer-ID definiert. Die Verwendung einer Personal-ID funktioniert je nach Benutzergruppe bzw. Accounttyp nicht. Dies hat zur Folge, dass sich die Benutzeraccounts in den Systemen nicht in jedem Fall eindeutig einem Mitarbeiter zuweisen lassen. Oder es existieren, vor allem in Legacy-Applikationen, unterschiedliche Regeln für Benutzer-IDs. Somit muss zuerst eine integrierte Sicht ("Korrelation") aufgebaut werden, die eine Beurteilung erlaubt, ob die IST-Berechtigungen eines Mitarbeiters den Regeln entsprechen.

Sind die Prozesse, Funktionen und Rollen der Applikationen definiert und initial vergeben, so braucht es einen regelmässigen, wenn möglich automatisierten Überprüfungsprozess, der sicherstellt, dass der Benutzer die richtigen Berechtigungen hat – und nur diese. Oft ist es der Vorgesetzte, der für seine Mitarbeiter die Rollen im Rahmen der Prozesse kennt, definiert und zuweist. Somit sollte der Vorgesetzte auch in den Überprüfungsprozess einbezogen werden. Bei der Prüfung von SOLL- und IST-Berechtigungen ist es wichtig, dass die IST-Berechtigungen wirklich dort analysiert werden, wo sie die Applikation bezieht. Dass angebliche IST-Berechtigungen in einem zentralen Directory durch lokale „Zusatzberechtigungen direkt in der Applikation“ ergänzt werden, ist keine Seltenheit und muss mitberücksichtigt oder noch besser verhindert werden.

Neben dem eigentlichen Ablauf des Überprüfungsprozesses muss definiert werden, wie oft eine Überprüfung stattfinden soll. Es muss also für jede Applikation eine Beurteilung der mit den Berechtigungen verbundenen Risiken erstellt werden. Hier besteht die Herausforderung darin, die Risiken zu identifizieren und zu beurteilen, da dafür das technische Verständnis sowohl der Applikationsfunktionalität als auch der beteiligten Geschäftsprozesse und Daten benötigt wird. Aufgrund der Risikoeinstufung kann dann entschieden werden, wie oft und in welcher Art eine Überprüfung stattfinden soll. Was die Aufgabe ebenfalls wesentlich erschwert, ist die Tatsache, dass insbesondere das "segregation of duties"-Prinzip applikationsübergreifend überprüft und durchgesetzt werden muss.

Die Mitarbeiter einer Firma durchlaufen bestimmte Prozesse automatisch, wodurch das Personalsystem oft ein sinnvolles Quellsystem ist. Hier existiert ein natürlicher Anknüpfungspunkt, um basierend auf dem Lebenszyklus des Mitarbeiters in der Firma auch Prozessschritte für die Accounts des Mitarbeiters zu definieren und idealerweise zu automatisieren. Für Accounts von externen Benutzern kann das Mitarbeitersystem aber keinen Input liefern. Hier müssen zusätzliche Prozesse definiert und umgesetzt werden, da auch die externen Mitarbeiter oder Personal von Lieferanten einem Lebenszyklus unterliegen. Wie bereits weiter oben erwähnt könnte hier ein Customer Relationship Management-System nützlich sein, das Kontaktangaben von Partnern und Kunden verwaltet. Alternativ kann mittels Föderierung auch eine direkte Echtzeitanbindung an Partnerfirmen geprüft werden.

Wenn privilegierte Accounts direkt einem Mitarbeiter zugewiesen und somit persönlich sind, gelten für sie dieselben Herausforderungen wie für die normalen Accounts. Für nicht persönliche privilegierte Accounts, und speziell für technische Accounts, besteht die Herausforderung vor allem darin, jeweils eine dafür verantwortliche Person zu identifizieren. Die Beurteilung der benötigten Berechtigungen ist oft auch nicht trivial, da die Grundlage dafür in der Applikationslogik versteckt sein kann.

Für Remote-Zugänge, vor allem im Kontext von Support durch einen Lieferanten, kann eine zeitlich begrenzte Freischaltung des Zuganges, wenn möglich gekoppelt mit einer Aufzeichnung aller Aktionen, die damit verbundenen Risiken massiv senken.

Eine Nutzung des Identity-Federation-Ansatzes, z.B. basierend auf dem SAML-Standard, kann aufwändige zentrale Überprüfungs- und Synchronisationsprozesse überflüssig machen, da damit verteilte Benutzerverwaltungsprozesse unterstützt werden.

Eine Nutzung von Token-basierter Authentisierung kann insbesondere Risiken im Bereich von technischen Accounts reduzieren.

Durchsetzung von Governance, Risk und Compliance (GRC)

Aus Sicht von GRC stellen Benutzeraccounts und Berechtigungen ein wichtiges Element für die Durchsetzung der firmenspezifischen Regeln dar. Regeln, die auf Risikobetrachtungen basieren und auf die Einhaltung von Regulierungen (Compliance) ausgelegt sind, bestimmen, welche Benutzer mit welchen Rechtekombinationen in welchen Prozessen arbeiten dürfen. Da eine vollständig automatisierte Durchsetzung dieser Regeln nicht immer wirtschaftlich sinnvoll umsetzbar ist, braucht es als Ergänzung üblicherweise auch manuelle Überprüfungen. Definition, Aufbau der Infrastruktur und Prozesse sowie Durchsetzung der Regeln sind je nach Komplexität der Informatik-Landschaft und der GRC-Anforderungen mit mehr oder weniger Aufwand verbunden.

Vorgehensmodell

Um im Bereich der Benutzeraccounts von einem unbekannten und unkontrollierten Zustand und den damit verbundenen Risiken und Kosten zu einem definierten, überprüfbaren Zustand zu kommen, hat sich folgendes Vorgehen bewährt:

1. **Analyse Ist-Zustand:** Der aktuelle Stand der Prozesse rund um Applikationen und Benutzerverwaltung wird analysiert. Der aktuelle Stand der Berechtigungen aller Applikationen wird analysiert. Daraus lässt sich ableiten, welche weiteren Schritte nötig sind.
2. **Anforderungen:** Definition der Anforderungen an Prozesse, Applikationen, Daten, einschliesslich einer Risikoklassifizierung
3. **Überprüfungen:** Durchführung und Etablierung von Überprüfungen, priorisiert nach Risiko.
4. **Bereinigung:** Bei den Überprüfungen identifizierte Fehler werden in den Applikationen korrigiert. Insbesondere werden unnötige Berechtigungen von den Accounts entfernt.
5. **Aufbau einer zentralen Benutzerverwaltung:** Mit einer zentralen Benutzerverwaltung werden die Prozesse unterstützt und eine zentrale Stelle geschaffen, in der alle Benutzerinformationen zusammengefasst sind.
6. **Aufbau einer rollenbasierten Berechtigungsvergabe:** Die Verwaltung von Berechtigungen mittels Rollen unterstützt die Durchführung von Reviews, schafft Transparenz und ermöglicht die Automatisierung der Rechtevergabe unter Einbezug der unterschiedlichen Account-Typen.
7. **Policies:** Basierend auf der zentralen Benutzerverwaltung und der rollenbasierten Berechtigungsvergabe können automatische Policies und Kontrollen, insbesondere zur Einhaltung von *Segregation of Duties*, etabliert werden.

Der wichtigste Erfolgsfaktor für eine nachhaltige und tragbare Benutzerverwaltungsinfrastruktur ist der Einbezug der Fachabteilungen, da es sich dabei nicht um ein reines Informatikthema handelt. Der Einbezug der Fachabteilungen muss frühzeitig erfolgen, damit die Teams und Vorgesetzten bei der Definition und Kontrolle der Berechtigungsprozesse mitwirken können. Entscheidend ist zudem, dass das Projekt von der Geschäftsleitung mitgetragen wird, da eine erfolgreiche Umsetzung sonst äusserst schwierig ist.

Fazit

Benutzerverwaltung ist einem ständigen Wandel unterworfen: Es werden neue Applikationen eingeführt, existierende Systeme erweitert oder die Konfiguration angepasst. Organisationsstrukturen werden verändert, Firmen fusioniert, Geschäftsprozesse angepasst oder Verantwortlichkeiten neu verteilt. All diese Veränderungen führen dazu, dass sich die Benutzer- und Rechteverwaltung in den Details laufend wandelt. Die Prozesse für die Benutzerverwaltung wie auch für die Überwachung müssen diesen Wandel ebenfalls berücksichtigen und abdecken. Die Verwaltung von Benutzern und die beschriebenen Vorgehensschritte sind mehr als nur ein einfaches Projekt. AdNovum hat verschiedenen Firmen dabei geholfen, eine erfolgreiche und kontrollierte Benutzerverwaltung mit den notwendigen Infrastrukturen aufzubauen. Dabei wurden die einzelnen Schritte in für die Firma und die Mitarbeiter verkraftbare Teile und Prozesse aufgeteilt und andererseits Verantwortlichkeiten etabliert, die eine ständige Weiterentwicklung und Verbesserung gewährleisten. Eine Investition, die sich auszahlt: Solche Firmen kennen ihre Benutzer.

Hauptsitz
AdNovum Informatik AG
Röntgenstrasse 22, CH-8005 Zürich
Tel. +41 44 272 6111
E-Mail: info@adnovum.ch

Geschäftsstelle Bern
AdNovum Informatik AG
Erlachstrasse 16b, CH-3012 Bern
Tel. +41 31 952 5858
E-Mail: info@adnovum.ch

AdNovum Singapur
AdNovum Singapore Pte. Ltd.
72 Anson Road, #07–01 Anson House
SG-079911 Singapore
Tel. +65 6536 0668
E-Mail: info@adnovum.sg

AdNovum Ungarn
AdNovum Hungary Kft.
Kapás utca 11–15, H-1027 Budapest
Tel. +36 1 487 5000
E-Mail: info@adnovum.hu