

Identity und Access Management für den Mittelstand

Entlastung für die Administration

von Thomas Reeb

Gerade in mittelständischen Betrieben stellen sich die IT-Verantwortlichen häufig die Frage, wie sie die regelmäßigen Arbeiten der IT-Administration vereinfachen und automatisieren können. Wir zeigen, wie ein richtig konzipiertes und eingesetztes Provisioning-System dabei helfen kann, dieses Ziel zu erreichen.

Infrastruktur ausbauen, Sicherheitskonzepte entwickeln, externe Standorte anbinden und neue Systeme implementieren: IT-Administratoren mangelt es nicht an wichtigen Aufgaben, doch viele dieser Arbeiten fressen Ressourcen, weil ihre Prozesse sehr zeitaufwändig sind. So genannte Provisioning-Systeme sollen deshalb die Administratoren bei der Versorgung von Mitarbeitern mit IT-Diensten und Zugriffsberechtigungen von Routineaufgaben entlasten. Zudem soll durch ihren Einsatz das Sicherheitsniveau erhöht werden. Doch der Mittelstand scheut sich nicht zu Unrecht vor der Einführung solcher Systeme: Sie sind üblicherweise für den Einsatz in Großunternehmen konzipiert und bekannt dafür, in unüberschaubaren Projekten mit ausufernden Kosten zu enden. Was bieten also spezielle Identity- und Access-Managementlösungen für den Mittelstand, und wie können sie der IT-Administration Arbeit abnehmen?

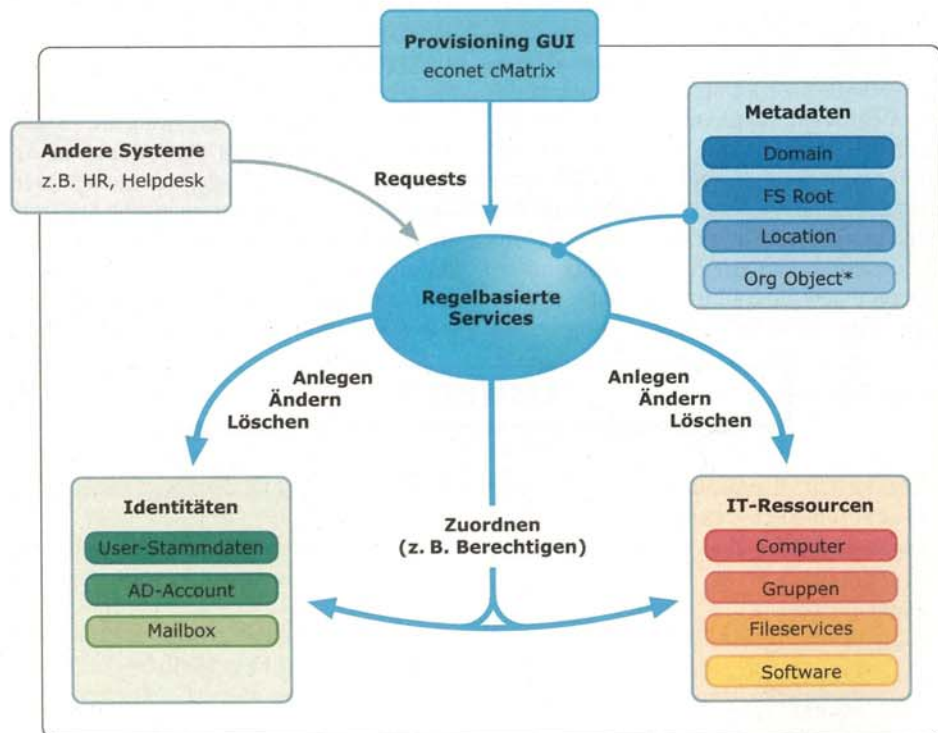
Die Administratoren in mittleren und kleineren Unternehmen setzen für die Abarbeitung von Standardaufgaben, wie dem Anlegen neuer Mitarbeiter in den Systemen, meist mehrere unterschiedliche Microsoft-Tools für die einzelnen aufeinanderfolgenden Aufgaben ein. Durch den hohen Anteil an Handarbeit entstehen bei einem derartigen Vorgehen nicht selten Fehleingaben, und Nachfragen sind an der Tagesordnung. Ein hohes Fehlerrisiko entsteht auch dadurch, dass mittelständisches IT-Personal oftmals mit zu vielen Rechten, wie beispielsweise Domain-Administrationsrechten, in den Zielsystemen arbeitet. Schnell ist hier statt einem einzelnen User eine ganze Organisationseinheit mit vielen Gruppen und hunder-

ten von Nutzern gelöscht. Grundsätzliche Prinzipien für die Rechtevergabe wie „Least Privilege“ und „Right Access to the Right People at the Right Time“ werden im Alltagsgeschäft leider oft ignoriert.

Vorteile des Provisionings: Automatisch den Überblick behalten. Mit einem Provisioning-System können die

Systembetreuer unterschiedliche Standard-administrationstätigkeiten von User- über Mail- bis hin zu Dateimanagement über eine Oberfläche erledigen. Das gilt für die vielen täglichen Änderungsanfragen und Aufgaben wie das Anlegen von Dateiablagen und die dazugehörige Vergabe und Verwaltung von Zugriffsrechten genauso wie für das Anlegen neuer Mitarbeiter in den Systemen. Die aufeinander folgenden Aufgaben sind in Prozessketten zusammengefasst und laufen nach bestimmten Vorgaben, die einmal definiert werden, regelbasiert und unter Zuhilfenahme von Metadaten automatisiert ab. Außerdem sind sie jederzeit in identischer Qualität reproduzierbar.

Wird zum Beispiel ein neuer Mitarbeiter bei der Anlage im Provisioning-System einer Abteilung – also ein User-Stammdatensatzes einem hierarchischen Strukturierungsobjekt – zugewiesen, ermittelt das System automatisch verschiedene Zugehörigkeiten. So „berechnet“ das Provisioning-System die Mitgliedschaft des Anwenders in den Default-Gruppen, die dieser Abteilung zugeordnet sind. Auch die Organisationseinheit im Active Directory, in der dieses Benutzerobjekt erstellt wird, sowie der zugehörige Exchange-Server für die Mailbox-Anlage werden ermittelt. Die Provisioning-Lösung setzt dementsprechend die erforderlichen Änderungen in den Zielsystemen um und



* Hierarchisches Strukturierungsobjekt

Bild 1. Identity Management kann auch für mittelständische Unternehmen erschwinglich und beherrschbar sein: Voraussetzungen dafür sind unter anderem ein fest definierten Umfang an Funktionen und Objekten und der Einsatz bewährter „Best Practices“ (Quelle: econet AG)

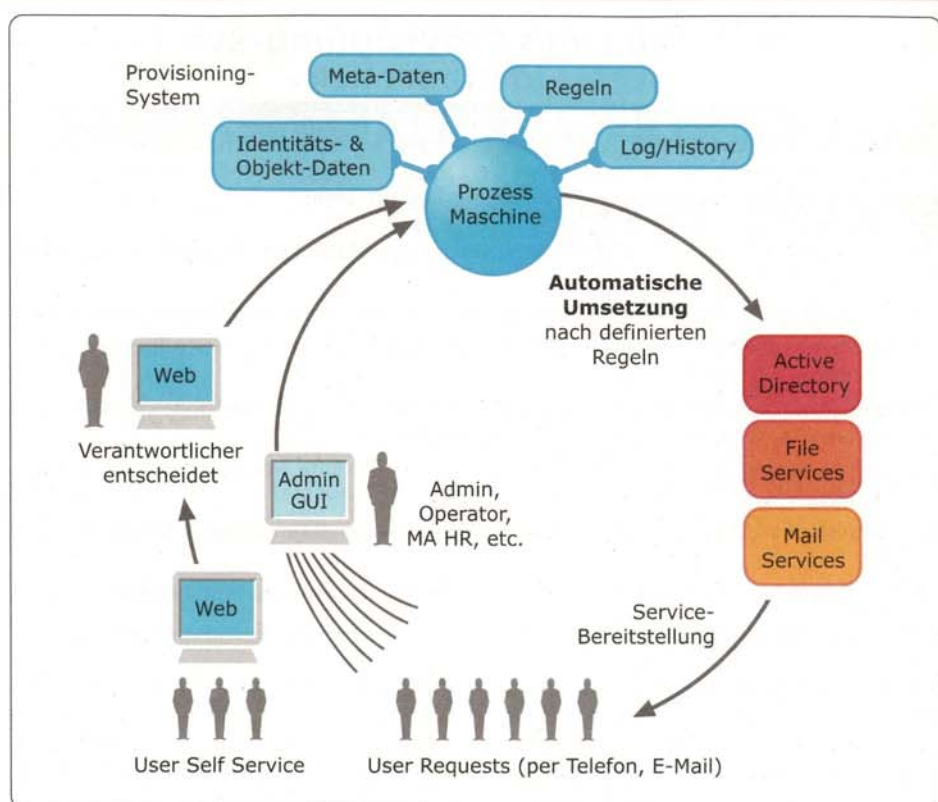


Bild 2. Die Prozessmaschine: Sie ist das Herzstück bei der Verwaltung von Identitäten und deren Berechtigungen beziehungsweise bei der Bereitstellung von IT-Diensten. Sie führt die gewünschten Änderungen automatisch und einheitlich nach hinterlegten Regeln aus. (Quelle: econet AG)

nimmt damit dem Administrator die Arbeit ab. So wird für den neuen Mitarbeiter in Abhängigkeit von der Fachgruppe oder der Abteilung vom System ein Account erstellt und in die richtigen Gruppen eingetragen. Zudem wird er automatisch mit entsprechend festgelegten Diensten versorgt, und erhält beispielsweise eine Exchange Mailbox und eine E-Mail-Adresse nach den unternehmensüblichen Namenskonventionen. Gleichzeitig wird jeder Zielsystem-Account einem Mitarbeiter zugeordnet. Unpersönliche Benutzerobjekte (Active Directory User Objects), für die keine Zuständigkeit ermittelt werden kann, sollten damit der Vergangenheit angehören. Da die für jedes zu provisionierende Objekt gilt, erhöht sich so auch die Transparenz.

Wichtiger Sicherheitsaspekt: Kein „Rechte-Chaos“ mehr. Mit einer geeigneten Provisioning-Lösung kann der mittelständische Administrator mit deutlich weniger direkten Rechten für die Zielsysteme arbeiten. Das System selbst, in dem er sich anmeldet, besitzt dann nur für jede Operation die entsprechenden Rechte. Da die Prozesse nach definierten Regeln ausgeführt und unter Zuhilfenahme von Metadaten umgesetzt werden, erfordern sie in der Regel auch nur ein Minimum an Eingaben. Das gestattet es

beispielsweise auch technisch ungeschulten Mitarbeitern, gleich nach der Erfassung der Stammdaten neuer Mitarbeiter Benutzer-Accounts und zugehörige Exchange-Mailbox anzulegen. Sie müssen dazu weder eine Vielzahl von Administrations-Tools bedienen, noch benötigen sie Expertenwissen in Sachen Active Directory. Da sich auch diese Mitarbeiter gegenüber der Provisioning-Lösung authentifizieren, brauchen sie zudem keine direkten Rechte in den Zielsystemen. Das IT-Personal kann außerdem auf diese Weise durch die Einführung von so genannten Self-Service Workflows weiter entlastet werden: Mit diesen Workflows beantragen Mitarbeiter IT-Dienste und Berechtigungen: Wird ein solcher Antrag vom zugehörigen Verantwortlichen in der Fachabteilung genehmigt, setzt das Provisioning-System die Änderungen automatisch in den Zielsystemen um. Diese standardisierten Genehmigungs-Workflows mit einem „Mehr-Augen“-Prinzip steigern das Sicherheitsniveau, indem sie helfen, die Umgehung der Richtlinien zur Rechtevergabe und unkontrollierte Freigaben zu verhindern.

Speicherung wichtiger Daten erhöht die Transparenz. Eine Identity- und Access-Managementlösung speichert alle Operationen, Prozesse und Prozessschritte

nachvollziehbar und transparent. Die Initiatoren behalten stets den Überblick über den Status ihrer Aufträge – egal, ob sich diese noch in der Warteschlange befinden, ob sie erfolgreich abgearbeitet sind oder sonstige Arbeitsschritte erfordern. Alle Operationen generieren automatisch Feedback für den Initiator oder auch den Bezieher des jeweiligen Services.

Auch in mittelständischen Unternehmen fordern immer mehr Gesetze und Regularien die IT-Verantwortlichen zum Handeln auf. Die meisten dieser Vorschriften laufen darauf hinaus, dass Unbefugte keinen Zugriff auf sensible Daten haben dürfen. Das hat natürlich auch eine Bedeutung bei der Auswahl eines geeigneten Identity- und Access-Managementsystems für das Unternehmen. So sollten Reporting- und Auditing-Funktionen in Provisioning-Systemen dediziert Auskunft über historisch gewachsene Rechte- und Dateistrukturen geben können. Gleichzeitig sollten sie aber auch Antworten bieten auf Fragen wie: Wer besitzt Rechte auf eine bestimmte Dateiablage im Unternehmen? Welche Rechte auf Datei-

nicht – auf einer serviceorientierten Architektur (SOA) basieren. Die Vorteile einer derart lose gekoppelten Architektur liegen allerdings auf der Hand: Das Unternehmen erhält

Vorteile eines Provisioning-Systems im Überblick

Richtig eingesetzt kann ein Provisioning-System auch den IT-Verantwortlichen in einem mittelständischen Betrieb viele Vorteile bieten. Sie werden durch eine ganze Reihe von Punkten entlastet und können sich so auf ihr Kerngeschäft konzentrieren:

- **Zuverlässigkeit:** Mitarbeiter werden schnell, verlässlich und standardisiert mit IT-Diensten versorgt.
- **Kein Chaos bei der Rechtevergabe:** Berechtigungen werden zentral vergeben und überwacht.
- **Sicherheit:** Verlässliche Absicherung von Geschäftsprozessen, regelbasierte Rechtevergabe und sicherer Rechteentzug.
- **Transparenz:** Umfassende Informationen über IT-Ressourcen, Zugriffskontrolle und Nachvollziehbarkeit zur Einhaltung von Compliance-Vorgaben.
- **Standardisierung:** Einheitliche Prozesse bei der Bereitstellung von IT-Services durch Best Practices.
- **Administration:** Entlastung und Senkung der Betriebskosten durch hohen Automatisierungsgrad.
- **Anwenderzufriedenheit:** Schnelle Servicebereitstellung und hohe Ausführungsqualität.

organisatorischen und strategischen Veränderungen im Unternehmen Schritt halten kann. Der Einsatz einer Provisioning-Lösung wie dem cMatrix Identity und Provisioning Manager der econet AG hilft, IT-Service-Prozesse zu standardisieren und zu automatisieren. Die Software, die speziell auf den Mittelstand zugeschnitten ist, beinhaltet dabei ein Set von Standardprozessen, mit denen die Mitarbeiter in den einzelnen Abteilungen sicher, zuverlässig und standardisiert mit den gewünschten IT-Diensten versorgt werden können. Optional steht ein Zusatzmodul mit Audit-Funktionen zur Verfügung, mit dem auf Knopfdruck Reports über Rechte- und Dateistrukturen erstellt werden können.

Abschließend zeigt sich, dass die Einführung eines derartigen Systems sowohl für die Anwender als auch für die Administratoren und das Management deutliche Vorteile bietet. Der Administrator ist durch die im System automatisch ablaufenden Prozesse entlastet und hat dennoch eine umfassende Dokumentation über alle erfolgten Vorgänge und deren nachvollziehbare sowie transparente Umsetzung. Der Anwender dagegen profitiert von einer schnellen Beantwortung seines Anliegens und einer ebenso raschen Umsetzung seiner Anforderungen. Für das Management zeigt sich in der Folge schnell, wie IT-Anfragen effizienter abgearbeitet werden, die Zufriedenheit mit der IT steigt und Kosten sinken. (fms)

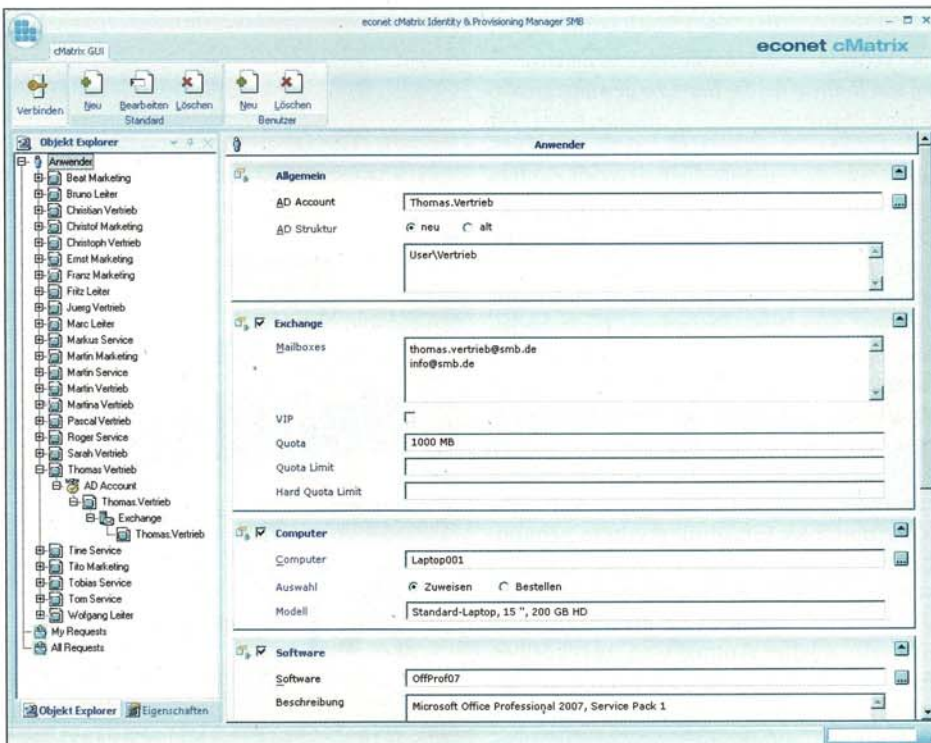


Bild 3. Eine Provisioning-Lösung im Einsatz: Dieser so genannte Identity- und Provisioning-Manager soll den Administratoren dabei helfen, IT-Prozesse zu standardisieren und automatisieren.

(Quelle: econet AG).

ablagen hat ein bestimmter Mitarbeiter? Welche Accounts oder Gruppen besitzen Zugriffsrechte innerhalb eines Fileservice? Das passende System sollte zudem eine Vielzahl diverser Services unterstützen. Ein Provisioning-System kann – muss aber

ein Werkzeug, das leicht um weitere Services erweitert werden kann. Beispiele sind Reporting-Services oder Self-Services. Darüber hinaus ist die einfache Integration einer solchen Lösung in bestehende Landschaften möglich. So ist garantiert, dass die IT mit den

Der Autor:

Thomas Reeb ist als Vorstand Marketing Sales bei der econet AG tätig.