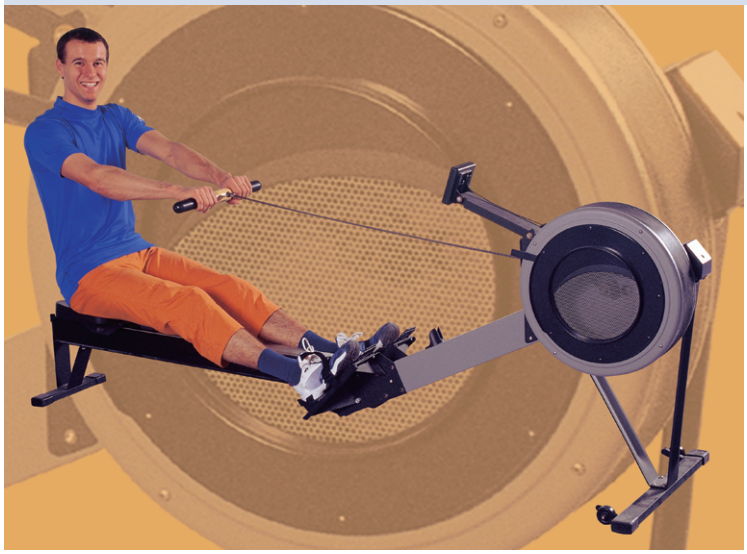
Administrationsaufgaben per Weboberfläche delegieren

Freizeitmaschine

Statt ihre kostbare Zeit mit lästigen Routineaufgaben zu vergeuden, lassen findige Admins die Benutzer selbst arbeiten. Neue Accounts anlegen oder die Gruppenzugehörigkeit ändern kann mit geeigneten Webformularen jeder User. Das Konzept und die Rechteverteilung müssen aber stimmen. Gottfried J. M. Grosshans



Gute Admins geben sich faul – sie lassen leidige Routinetätigkeiten von einem Skript erledigen und delegieren Aufgaben an die betroffenen Mitarbeiter. Diese begrüßenswerte Arbeitsscheu lässt dem versierten Systemverwalter mehr Zeit für interessante Aufgaben, erspart der Firma Kosten und den anderen Mitarbeitern bürokratischen Aufwand.

Neue User anlegen, Telefonverzeichnisse pflegen, Gruppenrechte ändern – diese typischen Admin-Arbeitsabläufe sind in einer kleinen Firma schnell erledigt. Sie summieren sich aber zu unübersichtlichen Zetteltürmen, auf denen Anwender ihre Änderungswünsche vermerken, wenn das Unternehmen auf mehrere Mitarbeiter-Hundertschaften anwächst. Dem Admin bleibt keine Zeit für die wichtigeren Aufgaben seiner Zunft.

Dieses Dilemma lässt sich vermeiden, wenn die Mitarbeiter ihre Änderungswünsche Skript-gesteuert selbst ausführen. Freilich wird sich kaum einer darauf einlassen, kryptische Befehle in die Shell zu tippen. Mittlerweile besitzt beinahe jede Firma ein Intranet mit eigenem Webserver. Es bietet sich an, einfache Webformulare mit den Admin-Skripten zu koppeln.

Die Freemail-Provider machen es seit Jahren vor: Jeder vernetzte Erdling kann dort selber einen Account beantragen und selbsttätig pflegen, ohne dass eine riesige Schar von Admin-Knechten beim Provider emsig die Arbeit erledigt. Ähnliche Systeme funktionieren auch innerhalb großer Institutionen – der Autor hat dies in einer Bank mit 3000 Mitarbeitern bewiesen.

Freemail als Vorbild

Die Benutzer waren begeistert, weil das System ihre Wünsche in Windeseile umsetzt. Kein Änderungsauftrag mehr, der nach dem Faxen an den Admin verloren ging oder Stunden und Tage auf Erledigung wartete. Kein neuer Mitarbeiter mehr, der tagelang ohne Zugangsberechtigung zum System und ohne Mail-Account auskommen musste.

In großen Institutionen ist die EDV-Landschaft meist sehr heterogen gestaltet, auch die Organisation und die internen Prozesse sind recht uneinheitlich. Keine Automatisierungssoftware wird daher jeder Firma, jedem Verein und jeder Universität gerecht. Die Prinzipien und Techniken gleichen sich dennoch, und mit etwas Skript-Entwicklung ist das perfekte System für die eigenen Anforderungen schnell fertig gestellt.

Vor der Implementierung sollte aber ein schlüssiges Konzept stehen, das sowohl technische Sicherheitsaspekte als auch die Firmen-Policy berücksichtigt. Ein Automatisierungsprojekt wird damit beginnen, die bisherige Prozessstruktur zu analysieren und zu beschreiben. Danach definiert es die Ziele, also den Zustand, der nach erfolgreicher Migration herrschen soll. Erst nach diesen Schritten beginnt die Implementierungsarbeit.

Die fiktive Firma Zettelwirtschaft AG will ihre Bereiche, Abteilungen und Gruppen (Abbildung 1) bei der Adminis-

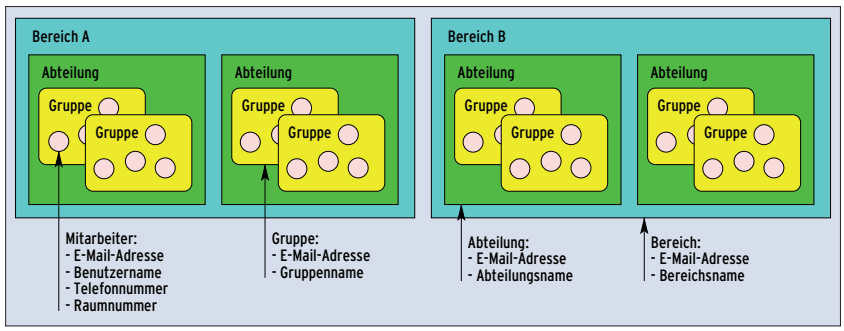


Abbildung 1: Die Zettelwirtschaft AG besteht aus zwei Bereichen, die Abteilungen und Gruppen enthalten. Jeder Mitarbeiter und jedes Element der Organisationsstruktur ist im Computersystem zu erfassen.

tration berücksichtigen. Während Abteilungen hierarchisch den Bereichen untergeordnet sind, lassen sich Gruppen nicht in die Hierarchie eingliedern. Sie können Mitarbeiter verschiedener Bereiche oder Abteilungen aufnehmen. Dieses Modell bildet auch typische Projektstrukturen ab.

Zettelwirtschaft AG

Bereiche, Abteilungen und Gruppen bestehen aus einem Leiter und beliebig vielen Mitarbeitern. Sie sind durch eindeutige Namen und eine Sammel-E-Mail-Adresse gekennzeichnet. Jeder Mitarbeiter der Zettelwirtschaft AG erhält eine eigene eindeutige Mailadresse, einen firmenweit eindeutigen Benutzernamen, eine Raumnummer und eine Telefonnummer.

Nach klassischem Muster muss der Administrator dieser Firma alle Mitarbeiter-Accounts selbst einrichten. Kommt ein neuer Kollege hinzu, ist wieder der Admin gefragt. In der Zettelwirtschaft AG muss der neue Angestellte das hauseigene Callcenter anrufen und ihm seine Wünsche und Daten mitteilen. Dort notiert ein Support-Mitarbeiter den Auftrag auf einem Zettel und faxt diesen an den zuständigen Admin. Der Admin administriert dann den oder die benötigten Server und Datenbanken. Nach Abschluss dieser lästigen Arbeit informiert er den Mitarbeiter.

Das gleiche Prozessschema gilt auch für das Modifizieren von Benutzerdaten, beispielsweise wenn sich ein Name ändert (Heirat oder Scheidung), die Firma in neue Räume umzieht oder ihre Telefonanlage umstellt. Selbst wenn der Mitarbeiter die Gruppe, die Abteilung, den Bereich oder das Projekt wechselt, ist dieser hohe Aufwand nötig. Abbildung 2 veranschaulicht die Prozesse.

Mehrere Medienbrüche stören den reibungslosen Ablauf, die Information muss zwischen unterschiedlichen Medien (Faxpapier, Telefon, Computer) durchgereicht werden. Dazu kommen mehrere Problemzonen. Kann der Admin zum Beispiel den neuen Mitarbeiter A nach erfolgter Administration nicht so-

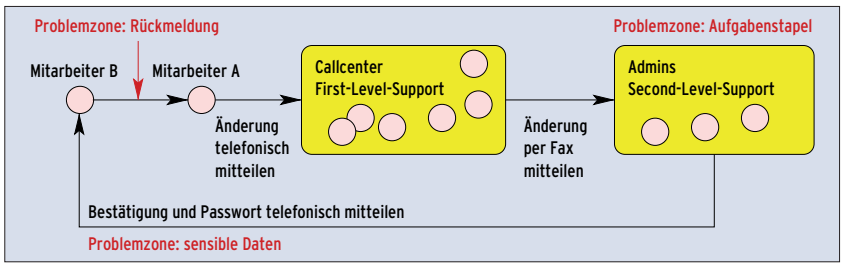


Abbildung 2: Der neue Mitarbeiter A ruft das Callcenter an, das den Auftrag an die Admins faxt, die den Account einrichten. Da sie A noch nicht erreichen können, informieren die Admins den Kollegen B. Diese Prozessstruktur ist durch ihre Medienbrüche (Telefon, Fax, Computer) sehr fehleranfällig.

- Anzeige -

fort telefonisch erreichen, muss er es weiter versuchen und dabei Zeit vergeuden. Nur so erfährt der neue Angestellte seine Zugangsdaten.

Im Prinzip könnte der Admin die Information einem Kollegen des betroffenen Mitarbeiters übermitteln. Dann weiß er allerdings nicht, ob Kollege B seinen Auftrag und die Daten nicht vielleicht vergisst. Außerdem kann er sensible Informationen (vor allem das Passwort) nicht einfach einem beliebigen Angestellten verraten. Zu allem Übel stapeln sich erfahrungsgemäß beim Administrator die Aufträge, da er für viele Aufgaben zuständig ist (Datensicherung, Serverwartung, Software-Installation …).

Der Aufwand führt zu einem entsprechend hohen Zeitbedarf. Tabelle 1 zeigt, wie lange ein typischer Vorgang dauert. Die linke Spalte führt die einzelnen Arbeitspakete auf, daneben sind der Aufwand in Minuten und die Wartezeit in Stunden vermerkt. Anrufen und ein Fax verschicken sind mit je zehn Minuten kalkuliert. Der Admin arbeitet sehr schnell und hat den Account in fünf Minuten angelegt. Vorher muss er aber dringendere Aufgaben erledigen – die zwei Stunden Wartezeit sind eher optimistisch, bei überlasteten Admins kann alles auch deutlich länger dauern.

Tabelle 1: Zeitaufwand vor der Migration

Vorgang	Arbeitsaufwand in Minuten	Wartezeit in Stunden	Vermerk
Mitarbeiter A ruft im Callcenter an	10	0	5 Minuten Gespräch, zwei Mitarbeiter (A und Admin)
Faxnachricht an die Admins	10	0	Faxblatt beschreiben und senden
Admin legt den Account an	5	2	Wartezeit wegen Aufgabenstapel
Admin telefoniert mit Mitarbeiter A oder B	10	0	5 Minuten je Mitarbeiter
Summe	35	2	

Tabelle 2: Rechteverteilung nach der Migration

Wer darf welchen Vorgang durchführen	MA	MA, Gruppe	MA, Abteilung	MA, Bereich
Eigenes Benutzerkonto anlegen/bearbeiten/löschen	✓	✓	✓	✓
Mitarbeiter zu Gruppe hinzufügen oder entfernen		✓		
Mitarbeiter zu Abteilung hinzufügen oder entfernen			✓	
Mitarbeiter zu Bereich hinzufügen oder entfernen				✓

Hoher Zeitaufwand

Die Firma muss mit 35 Minuten Arbeitszeit rechnen. Auch die zwei Stunden Wartezeit sind teuer, wenn der neue Angestellte in dieser Zeit nicht arbeiten kann. Technisch gesehen ist dieser Aufwand unnötig, wenn der neue Mitarbeiter seine Daten selbst eingibt und der Rest automatisch abläuft. Um Missbrauch zu vermeiden, muss aber Klarheit herrschen, wer genau welche Rechte vom Administrator übernehmen soll. Zudem ist es sinnvoll, alle Eingaben der Benutzer zentral zu protokollieren. Nur so lässt sich jederzeit feststellen, wer wann das System wie verändert hat. Im bisherigen Verfahren waren die Aktionen direkt nachvollziehbar, die Support-Mitarbeiter und Admins dürfen jetzt nicht die Übersicht verlieren.

Bei der Zettelwirtschaft AG sieht das Rechteschema nach der Migration wie in Tabelle 2 dargestellt aus. Jeder Mitarbeiter darf für sich selbst ein Benutzerkonto anlegen. Am eigenen PC ist das nicht immer möglich – vielleicht ist der Rechner noch gar nicht vorhanden oder der Mitarbeiter besitzt noch keine Zugangsdaten. In diesem Fall darf er sein Benutzerkonto auch am PC eines Kollegen einrichten. Danach kann er auch ohne eigenem PC schon E-Mail empfangen.

Nach dem Rechteschema aus Tabelle 2 dürfen alle Mitarbeiter einer Gruppe weitere Mitarbeiter in die Gruppe aufnehmen oder vorhandene Mitarbeiter löschen. Gleiches gilt für Abteilungen und Bereiche. Das Einrichten neuer Gruppen, Abteilungen und Bereiche ist nicht vorgesehen, hier ist noch der Administrator zuständig. Denkbar wäre es, auch diese Aufgabe den Mitarbeitern zu übertragen. Wer eine neue Gruppe (zum Beispiel für ein neues Projekt) anlegt, hätte zunächst exklusiv das Recht, weitere Mitarbeiter darin aufzunehmen. Jedes neue Mitglied der Gruppe würde das Recht erben, weitere Kollegen hinzuzufügen.

Ohne Formulare geht nichts

Für jede der berechtigten Aktionen ist ein Webformular nötig. Tabelle 3 zeigt diese Webseiten zusammen mit den Daten, die der Benutzer eingeben muss. Für jede Aktion ist eine Autorisierung (Berechtigung) mit vorangegangener Authentifizierung (Nachweis der eigenen Identität) nötig. Die einzige Ausnahme ist das Angelegen neuer Accounts – dies

Tabelle 3: Webformulare

Formular	Autorisierung erforderlich	Vorname	Nachname	Raum-Nr.	Telefon	Gruppe/Abteilung/Bereich	Benutzername/ Mitarbeiter
Benutzerkonto neu anlegen		✓	✓	✓	✓		
Benutzerkonto ändern	✓	✓	✓	✓	✓		✓
Benutzerkonto löschen	✓						✓
Mitarbeiter in Gruppe aufnehmen	✓					✓	✓
Mitarbeiter aus Gruppe entfernen	✓					✓	✓
Mitarbeiter in Abteilung aufnehmen	✓					✓	✓
Mitarbeiter aus Abteilung entfernen	✓					✓	✓
Mitarbeiter in Bereich aufnehmen	✓					✓	✓
Mitarbeiter aus Bereich entfernen	✓					✓	✓

ist jedem Mitarbeiter gestattet, auch dem neuen. Da er noch kein Benutzerkonto besitzt, kann er sich auch nicht authentifizieren. Aus Sicherheitsgründen darf der Zugang zu diesen Formularen nur intern möglich sein. Auch darf ein neu angelegter Account nicht zu üppig mit Rechten ausgestattet sein.

Der Lohn der automatisierten Version ist in Tabelle 4 zu sehen. Wartezeiten und Arbeitsaufwand reduzieren sich drastisch. Für ein monatliches Aufkommen von 100 Vorgängen waren vorher 58 Arbeitsstunden nötig, die Gesamtwartezeit hätte sich auf acht Tage summiert. Nach der Migration ist die Wartezeit gleich null und der Arbeitsaufwand beschränkt sich auf acht Stunden.

Die passenden Skripte

Bei der hohen Zeitersparnis lohnt es sich, etwas Arbeit in die Skripte zu investieren. Je nach Umgebung kann es leichter sein, eine fertige Lösungen wie Webmin [1] an die eigenen Anforderungen anzupassen oder eine eigene Lösung zu entwickeln. Die meisten Admins arbeiten bereits mit einer eigenen Skriptsammlung, die auf ihre IT-Umgebung abgestimmt ist. Sie um die passenden Webformulare ergänzen kann deutlich einfacher sein, als Webmin abzuspecken. Beide Varianten müssen wichtige Anforderungen erfüllen, unter anderem:

- Ergonomische Bedienung
- Datenredundanz vermeiden
- Rechteverteilung mit vorhandenen Systemen abbilden
- Temporäre Prozessdatenbanken vermeiden

Ergonomie betrifft vor allem die Gestaltung der Webseiten. Dazu zählt auch, dass Benutzer aussagekräftige Rückmeldungen vom System erhalten, nachdem sie einen Vorgang abgeschlossen haben. Diese Meldung muss auf jeden Fall klarstellen, ob es sich um einen Erfolg oder Misserfolg handelt, und in letzterem Fall verraten, wo es klemmt.

Datenredundanz dient dazu, das System so einfach wie möglich zu halten und von vornherein Fehler durch unnötige Komplexität zu eliminieren. Dazu zählen beispielsweise Konventionen für Benutzernamen und Mailadressen. Das Skript könnte beispielsweise beim Anlegen eines Accounts aus dem Vor- und Zunamen des Anwenders seine Mailadresse bilden, statt diese separat und unabhängig zu vergeben.

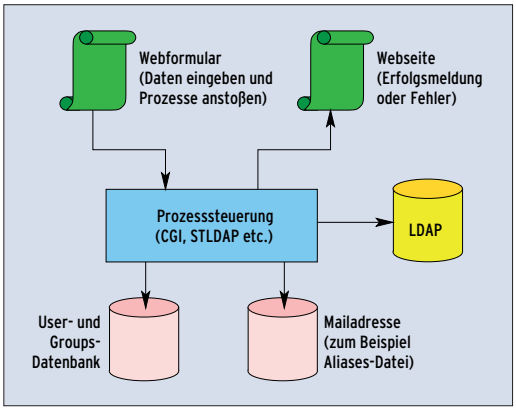


Abbildung 3: Nach der Umstellung automatisieren Webformulare und eine Prozesssteuerung wichtige Admin-Aufgaben. Die Skripte greifen direkt auf LDAP und die User-, Gruppen- und Aliases-Datenbanken zu. So bleibt den Admins mehr Zeit für wichtigere Aufgaben.

Eine sinnvolle Konvention wäre: Nimm den ersten Buchstaben des Vornamens, ergänze ihn durch einen Punkt und füge den Nachnamen an. Teste auf Redundanz (Name schon vorhanden). Bei Dopplern füge den nächsten Buchstaben des Vornamens ein. Bei identischen Vornamen dienen Ziffern zur Unterscheidung. Danach fehlen nur noch das @-Zeichen und der Domänenname.

Automatik im Detail

Die sechs Zettelwirtschaft-Mitarbeiter namens Jens Meier erhalten damit nacheinander die E-Mail-Adressen »J.Meier«, »Je.Meier«, »Jen.Meier«, »Jens.Meier«, »Jens.Meier2« und »Jens.Meier3«. Durch das Verfahren muss sich der Benutzer keine Gedanken über die Konvention machen. Das System arbeitet gerecht und nachvollziehbar.

Das Rechtesystem mit vorhandenen Systemen abzubilden vermeidet Autorisierungslücken. Beispielsweise sollten CGI-Skripte immer nur mit den Rechten der User laufen, von denen sie aufgerufen wurden. Ein Wrapper-Skript läuft dazu mit einem eigenen Account, dem keine zusätzlichen Rechte zugeteilt sind.

Hat sich der User im Webformular authentifiziert, wechselt der Wrapper mit »su -l *Benutzer*« in die Kennung des Benutzers, um dann beispielsweise per »passwd« das Passwort zu ändern. Wer eigene CGI-Skripte scheut und bereits einen Zope-Server und LDAP-Autorisierung per STLDAP-Manager [2] verwendet, kann die Rechtezuweisung auch weitgehend auf den STLDAP-Manager übertragen.

Temporäre Datenbanken vermeiden ist wichtig, um keine Kennwörter oder ähnlich kritische Daten im Klartext abzulegen. Das könnte boshaften Kollegen eine Angriffsfläche öffnen. Zudem muss das System so ausgelegt sein, dass mehrere Benutzer gleichzeitig ihre Änderungen durchführen können. Zusammenfassend ergibt sich das technische Prozessdiagramm aus Abbildung 3.

Letzte Hürde: Die Chefs

Jetzt müssen die sparwilligen Admins nur noch ihre Vorgesetzten davon überzeugen, die interne Firmen-Policy den ökonomischen Vorteilen unterzuordnen. Dies dürfte ihnen nicht schwer fallen, wenn sie sich mit guten Argumenten und den oben angeführten Zeitberechnungstabellen bewaffnen. *(fjl)*

Tabelle 4: Zeitaufwand nach der Migration

Vorgang	Arbeitsaufwand in Minuten	Wartezeit in Stunden	Vermerk
Mitarbeiter tippt Daten in das Webformular	5	0	Nur ein Mitarbeiter beteiligt
System erledigt Administration	0	0	
Mitarbeiter erhält Rückmeldung	0	0	
Summe	5	0	

Infos

[1] Webmin: [http://www.webmin.com]

[2] Gottfried J. M. Grosshans, „STLDAP-Manager – Zope verwaltet ein LDAP-Directory“: Linux-Magazin 05/04, S. 64