

-Modernisierung verständlich. Die Hauptgründe dafür sind allerdings nicht etwa zu hohe Entwicklungs- und Wartungskosten oder fehlende Programmierer-Ressourcen für die Legacy-Apps, sondern neue IT-Strategien und Zielarchitekturen. Laut Bosshard & Partner genügen die Altanwendungen den heutigen Anforderungen nach flexiblen Anpassungsmöglichkeiten an sich ändernde Geschäftsprozesse und -modelle schlicht nicht mehr. Vermehrt wird deshalb nach Integration, Interoperabilität und kürzeren Projektlaufzeiten gefragt. Daneben müssen die Unternehmen rasch auf wechselnde Kundenanforderungen reagieren – und dies möglichst kosteneffizient. Im heutigen Wettbewerb ist «Time to Market» mit schneller und flexibler Reaktion der IT auf neue Marktbedürfnisse überlebenswichtig. Über 70 Prozent der Studienteilnehmer sehen denn auch in erhöhter Produktivität und Kosteneffizienz die grössten Herausforderungen für die Applikationsentwicklung und -wartung.

Hohe Dringlichkeit für Software-Modernisierung

Die Studie belegt, dass sich die IT-Verantwortlichen diesen Herausforderungen stellen. Die Mehrzahl der be-

fragten Unternehmen hat im Rahmen ihrer IT-Strategien bereits konkrete Pläne. Über die Hälfte gibt an, Projekte für die Software-Sanierung und -Modernisierung heute auf ihrer Aktivitätenliste zu haben. Bei weiteren 17,3 Prozent sind entsprechende Vorhaben für die nächsten 3 bis 12 Monate traktandiert. Nur gerade 17 Prozent sehen diesbezüglich keine besondere Dringlichkeit.

Daraus wird deutlich, worum es geht: Die Legacy-Applikationen genügen aufgrund ihrer «monolithischen Bauweise» den heutigen Anforderungen nicht mehr. Waren bisher Robustheit, Zuverlässigkeit und Effizienz entscheidend, so wird heute vor allem Flexibilität und Interoperabilität gefordert.

Migration vor Neuentwicklung

Das Gros der befragten IT-Führungskräfte präferiert zwei Möglichkeiten für die Software-Sanierung und -Modernisierung: 78,5 Prozent den-

Die Mehrzahl der befragten Unternehmen wollen ihre Altapplikationen auf moderne Plattformen migrieren.

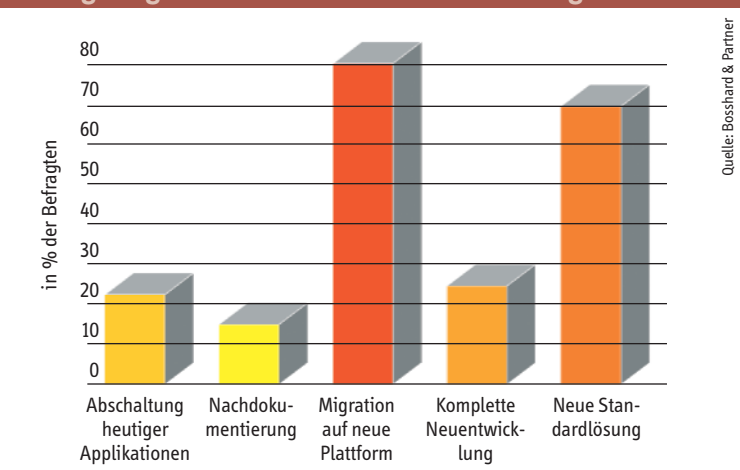
ken an eine Migration der Altanwendungen auf eine zeitgemässe Architektur, und 67,3 Prozent ziehen eine Ablösung ihrer Legacy-Software durch eine Standardlösung in Betracht. Überraschend abgeschlagen mit lediglich 26,2 Prozent werden komplette Neuentwicklungen erwogen.

«Bei der Migration der bestehenden Anwendungen auf moderne Applikationsarchitekturen werden die bewährten Systemfunktionen erhalten und gleichzeitig die Vorteile der besseren Integrationsfähigkeit der neuen Systemumgebung genutzt», erklärt Beat Berger, Autor der Studie

und Leiter Informatik Engineering bei Bosshard & Partner.

Zudem entfielen dabei die kostenintensive Umschulung der Anwender und Änderungen an der Ablauf- und Aufbauorganisation. Denn automatisierte Portierungen seien mit abschätzbarem Aufwand zu realisieren und die Funktionsfähigkeit der migrierten Applikationen könne mit Regressionstests zu 100 Prozent nachgewiesen werden. Dabei seien Kosten und Risiken wesentlich leichter abschätzbar und in der Regel geringer als bei der Einführung von Standardlösungen oder bei Neuentwicklungen, so Berger. ■

Lösungswege für die Software-Modernisierung



STEFAN WENGI – ARCHITEKTUR & ENTWICKLUNG



Mit IDM in eine Zukunft ohne Passwort

Identity Management (IDM) steht für die zentrale Verwaltung und Synchronisierung von Identitäten digitaler Nutzer inklusive Passwörtern und Zugriffsrechten. Wie vieles in der IT wurde auch diese Problematik bereits vor dem Aufkommen des Buzzword adressiert. Zum Beispiel hat man IDM als Enabler für Single Sign-on eingesetzt. Neben der Zentralisierung der Benutzeradministration zählen der Kostendruck, die Nachvollziehbarkeit von Mutationen auf Zugriffsrechte, gestiegene Sicherheitsanforderungen, regulatorische Bestimmungen und unternehmensübergreifende Informationsnutzung (Federated Identities) zu den Treibern. Insbesondere den Sicherheitsanforderungen, die integraler Bestandteil jedes IDM sein sollten, wird dabei meist zu wenig Gewicht beigemessen. Sicherheit muss gleichzeitig auf zwei Ebenen angegangen werden: im eigentlichen IDM-System als neuralgischem Angriffspunkt und in der unternehmensweiten Sicherheits-Architektur.

Die Einführung eines zentralen IDM geht deshalb mit der Überarbeitung oder der Definition von Prozessen einher wie etwa mit der Vergabe von Zu-

griffsberechtigungen. Ein weiterer Schwerpunkt ist die Integration bestehender Systeme. All das sowie die Komplexität bestehender Systemlandschaften führen dazu, dass der Aufwand für den Aufbau eines IDM beträchtlich ist. Die Erfolgsfaktoren eines IDM-Projekts sind demgegenüber rasch aufgezählt:

Die «weichen» Faktoren zuerst:

■ Meist sind viele verschiedene Organisationseinheiten und Personen betroffen. Damit die Zusammenarbeit klappt und dem Unterfangen gebührend Priorität beigemessen wird, muss das Projekt vom obersten Management getragen werden.

■ Der Projektleiter sollte nicht nur ein vertieftes technisches Security- und IT-Architektur-Know-how haben, sondern gleichzeitig über ausserordentliche Kommunikations- und Integrationsfähigkeiten sowie Durchsetzungskraft verfügen.

Hinzu kommen die harten Faktoren:

■ Damit Stammdaten automatisch übernommen werden können, ist eine Anbindung an das HR-System anzustreben, um Ein- und vor allem Austritte erkennen zu können.

- Die Integration von bestehenden Systemen und Sicherheitskonzepten muss Projektbestandteil sein.
- Damit ein IDM-System zum Baustein einer zukunftsgerichteten Gesamtarchitektur werden kann, sollte es als fixer Bestandteil der «Security Service Architektur» positioniert werden; beispielsweise mit der Anbindung an bestehende Directories oder Authentisierungsdienste.

Bereits heute kann man neben Benutzeridentitäten auch jene von Rechnern, Applikationen und Services verwalten. Denkt man das Konzept weiter, könnte sich IDM in Zukunft zu einem ganzheitlichen Informationssystem entwickeln, das die produktive Systemlandschaft widerspiegelt und das etwa das heute weit verbreitete Führen von relevanten Informationen in Spreadsheets überflüssig macht.

Die meisten verfügbaren IDM-Produkte befassen sich aber noch vorwiegend mit der Synchronisation von Passwörtern. Innovative Ansätze gehen jedoch darüber hinaus. Passwörter sollen künftig nicht mehr synchronisiert, sondern abgeschafft und durch eine Authentisierung auf der Basis von «Security Hardware Token» ersetzt werden. IDM kann sich dann auf seine zentralen Aufgaben konzentrieren, nämlich Identitäten zu verwalten und Zugriffsrechte zu vergeben.

STEFAN WENGI IST CTO DES ZÜRCHER SOFTWAREHAUSES ADNOVUM INFORMATIK.
STEFAN.WENGI@ADNOVUM.CH