IT Risikomanagement
in Integrationsprojekten

NETZGUIDE Ausgabe Mai 2009

IT-Risikomanagement in Integrationsprojekten

Integrationsprojekte machen Geschäftsprozesse effizienter. Gleichzeitig erhöhen sie die Abhängigkeit einer funktionierenden Informatik. Dies erfordert ein Risikomanagement in den Projekten und standardisierte Richtlinien in der Softwareentwicklung. Martin Dietrich, Thomas Keller

Martin Dietrich
ist Sicherheitsexperte und verantwortlich für die BINT Methodik, BINT GmbH

Thomas Keller
ist Leiter Zentrum für Wirtschaftsinformatik ZHaW und Leiter Softwareentwicklung, BINT GmbH

Durch Integrationsprojekte sollen Geschäftsprozesse automatisiert, Daten aus verschiedenen Quellen zusammengeführt oder Entscheidungsgrundlagen verbessert werden. Nachdem heute die abteilungsinternen Prozesse, dank entsprechender Software, effizient ablaufen und der Datenfluss weitgehend geregelt ist, verlagert sich der Fokus zunehmend auf abteilungs- und unternehmensübergreifende Geschäftsprozesse. Diese Ziele werden vor allem durch die Standardisierung von Abläufen, die Abschaffung von Medienbrüchen, die Automatisierung im Datenaustausch und der Datenkonversion erreicht. Dies führt aber unweigerlich auch zu Nebenwirkungen wie zum Beispiel:

- Reduktion der manuellen Datenkontrolle, erhöhte Abhängigkeit der Datenverfügbarkeit und deren Qualität oder Transparenzverlust bezüglich der Datenherkunft.
- Auswirkungen von Störungen in der Informatik sind nicht mehr auf eine Abteilung beschränkt, sondern wirken sich sofort auf weitere Abteilungen, das ganze Unternehmen oder sogar auf ganze Wertschöpfungsketten aus.
- Es kommen neue IT-Komponenten zum Einsatz (zum Beispiel Datentransport- oder Datenkonvertierungssysteme, Auskunftssysteme, zentrale Authentifizierungsdienste und Autorisierungsstellen), die neue Risiken (wie Ausfall des Transportweges, Korruption der Daten) mit sich bringen können. Somit ist schnell ersichtlich, dass Integrationsprojekte neben der erwünschten Effizienz- und operativen wie strategischen Entscheidungsvorteilen auch eine neue Risikoexposition mit sich bringen.

Neue IT-Komponenten bringen neue Risiken

Da die gewünschten Vorteile der Integrationsprojekte die erwähnten Auswirkungen auf die Risikoexposition mit sich bringen, können diese nicht einfach gelöst, sondern müs-

Schutzbedarf	1	2	3	4
Testkonzept Komponenten-Integration	Level Test Plan Level Test Design Level Tests Case Level Test Procedure Level Test Log Level Interim Test Status Report Level Test Report	Schutzbedarf Stufe 1 + Anomaly Report	Schutzbedarf Stufe 2 + Master Test Plan Master Test Report	Schutzbedarf Stufe 3

Abbildung 1: Aus der Schutzbedarfsanalyse abgeleitete Anforderungen am Beispiel «Testkonzept»

sen entsprechend gemanagt werden. Das projektspezifische Risikomanagement liegt in der Verantwortung des Gesamtprojektleiters. Er ist dafür verantwortlich, dass die veränderte Risikoexposition im Projekt analysiert und die entsprechenden Massnahmen frühzeitig geplant und umgesetzt werden. Es genügt nun aber nicht, den Projektleitern diese Aufgabe zu übergeben. Vielmehr muss man ihnen die zur Aufgabenerfüllung notwendigen Ressourcen (wie Know-how, Hilfsmittel, Checklisten) zur Verfügung stellen und das Risikomanagement aktiv überwachen.

Vorgehen in der Praxis anhand dreier Kernaufgaben

In der Praxis hat sich ein Vorgehen bewährt, das um drei Kernaufgaben kreist: die Identifikation des Schutzbedarfs der Geschäftsprozesse; die Ableitung der Anforderungen an die Sicherheitsvorkehrungen und die Umsetzung vordefinierter, standardisierter Sicherheitsmassnahmen.

- Der Schutzbedarf eines Geschäftsprozesses wird mittels eines sogenannten Risikodialogs erhoben. In einem Interview mit den Geschäftsprozessverantwortlichen werden unter Anwendung der Szenariotechnik die möglichen Auswirkungen von Informatikstörungen identifiziert. Dabei geht es nicht nur um die – normalerweise schwer bezifferbaren – finanziellen Auswirkungen, sondern ebenfalls um Auswirkungen in den Bereichen Imageverlust, Beeinträchtigung der Aufgabenerfüllung, rechtliche Folgen oder Auswirkungen auf Personen. Dabei werden Störungen in den vier Dimensionen Verfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit betrachtet. Der Fokus des Risikodialogs liegt bei den unternehmensseitigen Auswirkungen von Informatikstörungen, nicht bei technischen Details oder Abschätzung von Wahrscheinlichkeiten. Bei Integrationsprojekten speziell zu beachten ist, dass die Geschäftsprozesse richtig abgegrenzt und alle involvierten Abteilungen und/oder Unternehmen insgesamt betrachtet werden. Die Kooperation, die auf Prozessebene angestrebt wird, muss sich auch im Risikomanagement, zumindest bezüglich der gemeinsamen Prozesse, etablieren.

> «Die möglichen Auswirkungen von Informatikstörungen werden in einem Interview mit dem Geschäftsprozessverantwortlichen ermittelt.»

- Aus den Resultaten der Schutzbedarfsanalyse sind die notwendigen Massnahmen abzuleiten. Dabei lassen sich grundlegende Architekturentscheide und die konkrete Umsetzung mit den detaillierten technischen Fragestellungen unterscheiden. Die Schutzbedarfsanalyse gibt also Inputs bezüglich architektonischen Entscheidungen wie Hardwarekonfiguration (einzelner Server, Cluster, weitere Redundanzen), Datensicherung (Backup-Restore, Datenspiegelung), Authentifizierungskonzepte (Token, Zertifikate, Username und Passwort) oder Datenverschlüsselung (wie verschlüsselte Speicherung, verschlüsselter Transport intern/extern, Daten auf Laptop). Bei unternehmensübergreifenden Projekten lassen sich in dieser Aufgabe oft einfachere und mit tieferen Kosten verbundene gemeinsame Lösungen finden.
- Die dritte Kernaufgabe besteht darin, die in der Schutzbedarfsanalyse ermittelten Anforderungen und die daraus abgeleiteten Architekturmassnahmen im Projekt umzusetzen. Dieses Spektrum reicht von der Unterstützung der geforderten Architekturen (Redundanzen, Verschlüsselung, Authentifizierung) über die Einhaltung detaillierter Programmierrichtlinien bis zu schutzbedarfsabhängigen Testverfahren.

Diese drei Kernaufgaben werden im Verlaufe des Projektes immer wieder angegangen, überprüft und konkretisiert. Zum Investitions- und/oder Projektantrag gehört bereits eine erste Schutzbedarfsanalyse. Denn die darauf aufbauenden Architekturgrundsätze können erheblichen Einfluss auf die prognostizierten Umsetzungskosten haben. Bei der Erarbeitung des Pflichtenhefts müssen die ursprüngliche Schutzbedarfsanalyse aktualisiert und die daraus abgeleiteten Anforderungen aufgenommen werden. Bei der Evaluation der angebotenen Lösungsvarianten müssen auch die sicherheitstechnischen Vorkehrungen berücksichtigt werden. Während der Projektrealisierung werden die Geschäftsprozesse laufend konkretisiert. Daraus können erneut Anpassungen an die Auswirkungen von Informatikstörungen auf die Geschäftsprozesse resultieren. Deswegen muss die Schutzbedarfsanalyse auch in dieser Phase überprüft und gegebenenfalls aktualisiert werden. Hier ist es zusätzlich wichtig, dass die Umset-

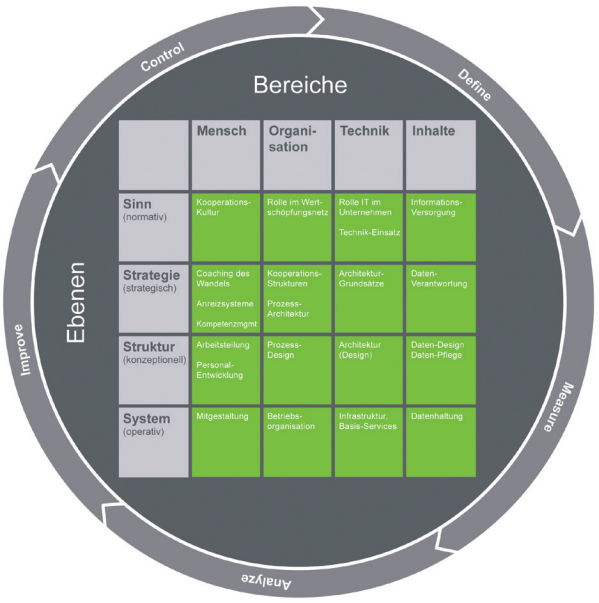

Abbildung 2: Ein Framework für Integrationsprojekte

zung der vorher definierten Massnahmen verifiziert wird. Es ist durchaus möglich, dass einzelne Massnahmen nicht wie geplant umgesetzt werden können. In diesem Fall greift das Risikomanagement erneut und definiert mögliche notwendige Ersatzmassnahmen.

In der Theorie ist das Vorgehen also bestens bekannt. Leider jedoch spiegelt die Praxis und die täglichen Erfahrungen im Umgang mit Unternehmensapplikationen eine andere Welt. Aus einer erst kürzlich erschienen Arbeit der Mitre Corporation über die Top 25 gefährlichsten Programmierfehler ist ersichtlich, dass im Sicherheitsbereich noch sehr viel Optimierungspotenzial vorhanden ist: die Klartextübertragung sensitiver Informationen, die Fehlermeldungen mit sensitivem Inhalt, ungeeignete Authorisierungsverfahren, hart-codierte Passwörter und die Benutzung ungenügender kryptographischer Verfahren.

Es stellt sich nun die Frage, wie dieser Gap zwischen dem theoretischen Wissen und der gängigen Praxis geschlossen werden kann. Ein Weg ist die Entwicklung eines eigenen Frameworks und darauf beruhender Methoden, Spezifikationstemplates, Checklisten und weiterer Hilfsmittel für Projektleiter wie für Entwickler.

Standardisiertes Framework bringt umfassenden Nutzen

Ein solches Framework sollte neben den typischen Themen des Software-Engineerings auch die Sicherheitsaspekte umfassend berücksichtigt werden. Ausserdem sollte dabei der gesamte beschriebene Prozess unterstützt und die Resultate der Schutzbedarfsanalyse direkt in entsprechende Anforderungen an die Softwareentwicklung sowie an das Testkonzept umgesetzt werden. Der Nutzen aus der vorgestellten Vorgehensweise und der Anwendung eines standardisierten Frameworks ergibt sich in verschiedenen Bereichen: Benutzer und Prozessverantwortliche werden besser in das Projekt integriert, die notwendigen Sicherheitsmassnahmen werden frühzeitig geplant und die prognostizierten Projektkosten werden realistischer. Für die umzusetzenden Sicherheitsmassnahmen existieren standardisierte Vorgaben – jedes Projekt wird mit dem gleichen Massstab gemessen. Die Gefahr nachträglich anfallender Kosten für die Erhöhung des Sicherheitslevels ist um ein Vielfaches kleiner. Die Qualität der Softwareentwicklung ist prüf- und nachvollziehbar und die Softwareentwicklung wird standardisiertert.

Abbildung 3: Mithilfe eines Tools kann eine Schutzbedarfsanalyse erstellt werden.

BINT GmbH • Business Integration
Hard 5 • CH-8408 Winterthur • Telefon +41 52 223 21 85 • Fax +41 52 223 21 86 • info@bint.ch • www.bint.ch