

Von der Methode zum Prototypen

Werkzeuge zur Modellierung der Unternehmensarchitektur (Enterprise Architecture Tools) adressieren dieses Problem, indem sie die Speicherung der relevanten Informationen in strukturierter Form ermöglichen und in verschiedenen Darstellungsformen bereitstellen. Ein EA-Tool besteht in der Regel aus drei wesentlichen Komponenten:

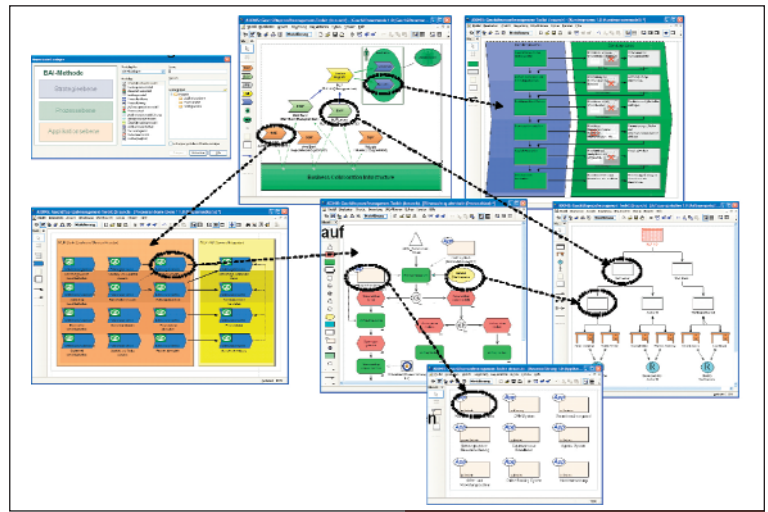
- ▶ Datenbank zur Speicherung aller Einzelinformationen der Geschäftsstrategie, der Geschäftsprozesse, der Organisation und der sie unterstützenden Applikationen.
- ▶ Metamodell zur Definition und Strukturierung der relevanten Informationen, die in der Datenbank gespeichert werden sollen.
- ▶ Oberfläche zur Modellierung und Präsentation der gespeicherten Informationen in grafischer und textueller Form.

Im Kompetenzzentrum «Bankenarchitekturen im Informationszeitalter» des Instituts für Wirtschaftsinformatik der Universität St. Gallen (CC BAI) wurde in Zusammenarbeit mit Partnerunternehmen aus dem Finanzdienstleistungssektor eine Methode zur Gestaltung der Unter-

nehmensarchitektur entsprechend den Grundsätzen des Business Engineering entwickelt.

Die Methode umfasst auf jeder der drei Gestaltungsebenen «Geschäftsstrategie», «Organisation» und «Informationssystem» Vorgehensmodelle, Aktivitäten und Spezifikationstechniken. Um die Zusammenhänge zwischen den drei Ebenen abzubilden, basiert die Methode auf einem ebenenübergreifenden Metamodell. Das Ziel der Methode liegt in einer breiten Darstellung der Schlüsselemente eines Unternehmens ohne Fokus auf softwareentwicklungsrelevante Aspekte. Das ebenenübergreifende Metamodell dient der konsistenten Abbildung aller Artefakte, die für Entscheidungen im Schnittbereich von Fachbereich und IT relevant sind (Leistungssystem, Zielsystem, Prozesse, Organisationseinheiten und Applikationen), sowie deren Zusammenhänge.

Da es nicht möglich ist, alle Artefakte in einem Totalmodell abzubilden und ausreichend zu pflegen, wurde bei der Entwicklung der Methode versucht, einen sinnvollen Aggregationsgrad zu erreichen. Um die Umsetzbarkeit und Anwendbarkeit der Methode zu illustrieren,



Screenshot des Softwareprototypen der Uni St. Gallen.

wurde diese in dem Metamodellierungswerkzeug ADONIS der Firma BOC Information Objects Consulting abgebildet, welches auf einem weitgehend methodenunabhängigen Metamodellierungsansatz basiert und somit eine leichte Anpassung der zugrundeliegenden Metamodelle ermöglicht.

Der daraus entstandene Software-Prototyp liegt nun in einer ersten Version (siehe Abbildung oben) vor und kann in der Unternehmenspraxis zu Testzwecken für einen beschränkten Zeitraum kostenlos genutzt werden – unter der Voraussetzung,

dass der Prototyp konkret in einem EA-Projekt verwendet wird und die Erkenntnisse aus dem Einsatz für die Weiterentwicklung des Prototyps sowie für unsere wissenschaftliche Arbeit genutzt werden können.

CHRISTIAN BRAUN IST WISSENSCHAFTLICHER MITARBEITER AM INSTITUT FÜR WIRTSCHAFTSINFORMATIK (IWI) AN DER UNIVERSITÄT ST. GALLEN; ROBERT WINTER IST PROFESSOR UND DIREKTOR DES IWI.

ARCHITEKTUR & ENTWICKLUNG: STÉPHANE MINGOT



Sicherheit ohne Ende

Ohne Sicherheit kein reibungsloses E-Business. Konzentrierte man sich bisher darauf, den externen Zugang zu schützen, muss eine moderne Sicherheitsarchitektur alle relevanten IT-Aspekte abdecken, wobei Anwender einen durchgängigen und trotzdem einfachen Zugang zu Applikationen und Daten haben sollen. Das bedingt jedoch, dass dem Endbenutzer via Secure Reverse Proxy (Entry Server) über alle Knoten hinweg bis zum Mainframe eine lückenlose, einheitliche Sicherheitskette gewährleistet wird. Identität und Rechte sollen entlang der gesamten Kette so propagiert werden, dass bei jedem Knoten automatisch geprüft werden kann, auf welche Funktionen oder Daten der Anwender zugreifen darf. Zusätzlich lassen sich seine Operationen dank einer Prüfspur über alle Knoten nachvollziehen. Dies ist das Konzept von E2E-Security (End-to-End).

E2E-Security wird allerdings selten konsequent und durchgehend umgesetzt. Zurückzuführen ist das auf unzureichendes Know-how bei der Integration, ungenügende Flexibilität der Software und eine Unterschätzung der technischen und organisatorischen Implikationen.

E2E-Security-Lösungen sind prinzipiell Integrationsprojekte und bei jedem Kunden anders, denn es müssen jeweils die unterschiedlichsten Komponenten optimal miteinander zusammenspielen. So gilt es meistens, heterogene Clients auf verschiedenen Betriebssystemen in Kombination mit heterogenen Anwendungsplattformen abzusichern. Zudem gelangen in der Regel unterschiedliche Authentisierungsverfahren wie zertifikatsbasierte Authentisierung, Challenge/Response, One-Time-Passwort und Raster-Karte mit verschiedenen Security Devices zum Einsatz.

E2E-Security ist dabei nicht nur eine vertikale, sondern auch eine horizontale Integration. Die Lösung sichert also mehrere Anwendungen so ab, dass sie geschützt kommunizieren und gemeinsame vertrauenswürdige Services nutzen können. Das bietet Erleichterungen für Anwender wie Single Sign-on sowie für Revisoren in Form eines zentralen Auditservers. Das heisst aber auch, dass man die Anwendungen an zentrale Services wie ein Identity-Management-System, eine PKI oder ein Zertifikatmanagementsystem anbinden muss.

Diese zentralen Dienste sind oft nicht oder nur teilweise vorhanden und müssen gebaut und als Baustein des Gesamtsystems integriert werden. Die Architektur muss deshalb flexibel sein. Um alle

Knoten anzubinden, benötigt man zudem einen so genannten Security Stack. Dieser besteht aus voneinander unabhängigen und modular zusammenstellbaren Komponenten, die für den Zugriff auf lokale Credentials (Sicherheitsmerkmale wie private Schlüssel), die Etablierung verschlüsselter Verbindungen zwischen zwei Knoten und die Propagierung der Identitäten verantwortlich sind. Bei unserem Sicherheitsprojekt bei der UBS etwa wurde der Nevis Security Stack über zwölf Betriebssysteme hinweg ausgebreitet, womit eine durchgängige E2E-Security-Lösung entstand.

Da der Nevis Security Stack einfach zu portieren und modular einsetzbar ist, garantiert er auch, dass die E2E-Security in mehreren Schritten erfolgen kann und folglich bei jedem Projekt eine sanfte Migration möglich ist. Die Verwendung offener Standards macht es möglich, bestehende Komponenten für die Migration oder auch dauerhaft in eine Lösung einzubetten.

Eines muss bei einem E2E-Security-Projekt von Anfang an klar sein: Angesichts der technischen und vor allem organisatorischen Implikationen kann es nur Bestandteil eines gesamten IT-Konzepts sein und muss deshalb auf Management-Stufe initiiert und geleitet werden.

STÉPHANE MINGOT IST SENIOR PROJECT MANAGER BEI ADNOVUM INFORMATIK AG. STÉPHANE.MINGOT@ADNOVUM.CH