Auf einen Blick

Bei der Koppelung von Anwendungssystemen muss neben der Integration der Funktionalitäten der Ausgangssysteme auch die dort verwendete Sicherheitsarchitektur verbunden werden. Hierbei ergeben sich Probleme aufgrund verschiedenster Sicherheitsansätze: z.B. im Zugriffskontrollsystem, Passwortmanagement oder Verschlüsselungstechnik. Ziel dieses Teilprojektes ist die Definition einer einheitlichen Sicherheitsplattform zur kompletten Auslagerung in einen sogenannten Security-Server.

Status

laufendes Projekt

Kontakt

Prof. Dr. Dieter Bartmann
Universität Regensburg
Lehrstuhl für Wirtschaftsinformatik II
93040 Regensburg

Telefon ++49 (0)941/943-1881
Telefax ++49 (0)941/943-1871
E-Mail bartmann@forwin.de

FORWIN: Kompetenz made in Bavaria

Im Bayerischen Forschungsverbund Wirtschaftsinformatik (FORWIN) bearbeiten acht nordbayerische Lehrstühle der Wirtschaftsinformatik an fünf Universitäten (Bamberg, Bayreuth, Erlangen-Nürnberg, Regensburg, Würzburg) gemeinsam Probleme, die sich aus der Kopplung der elektronischen Informationsverarbeitung (IV) über die Grenzen einzelner Betriebe hinaus ergeben. Dazu zählen E-Business, die Abstimmung der EDV zwischen Unternehmen, die in einer Lieferkette operieren (Supply Chain Management), und die Entwicklung von IV-Systemen aus Software-Bausteinen, die an ganz unterschiedlichen Stellen produziert worden sind.

FORWIN hat sich zum Ziel gesetzt, in diesem Umfeld in enger Kooperation mit einer Reihe von Unternehmen innovative Lösungen zu entwickeln und nicht zuletzt aktuelle wissenschaftliche Erkenntnisse und praktische Erfahrungen in die Ausbildung einfließen zu lassen.

Geschäftsführung, Zentrale, Information

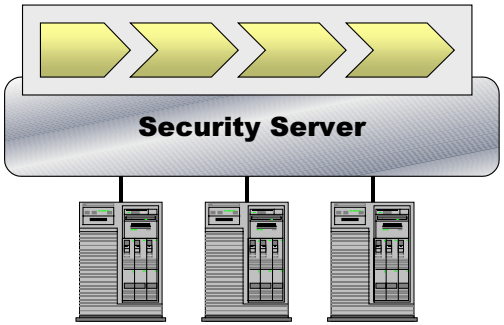
Bayerischer Forschungsververbund
Wirtschaftsinformatik
Äußerer Laufer Platz 13/15
90403 Nürnberg

Telefon: ++49 (0)911/5302-151
Telefax: ++49 (0)911/5302-149
Internet: http://www.forwin.de

Bayerischer Forschungsverbund Wirtschaftsinformatik
Lehrstuhl Prof. D. Bartmann

High-Tech-Offensive Zukunft Bayern

Sicherheitsintegration bei der Anwendungssystemkoppelung



forwin

BAYERISCHER FORSCHUNGSVERBUND WIRTSCHAFTSINFORMATIK
BAMBERG • BAYREUTH • ERLANGEN-NÜRNBERG • REGENSBURG • WÜRZBURG

Sicherheitsintegration bei der Anwendungs-systemkoppelung

Ausgangssituation

Die zur Erbringung von Bankdienstleistungen notwendigen Prozesse laufen derzeit weitgehend isoliert voneinander in verschiedenen Anwendungssystemen (AWS) ab (z. B. bei der Baufinanzierung: Verkauf einer Lebensversicherung und eines Bausparvertrages, Gewährung eines Hypothekendarlehens sowie eines Bereitstellungskredits, Einräumung eines Dispositionskredits). Hier entstehen immense Effizienz- und Effektivitätsverluste. Ziel ist es, eine Anwendungsintegration über Systemkoppelung so zu erreichen, dass (Teil-)funktionalitäten eines AWS auch von einem anderen AWS genutzt werden können.

Reiht man die Einzelfunktionen eines AWS gedanklich in einer Kette aneinander, so bedeutet Systemkoppelung, dass bei der Bearbeitung eines konkreten Geschäftsvorfalles Seiteneinstiege von einer AWS-Kette in eine andere geschehen. Im Extremfall hangelt sich der Benutzer in Hypertext-Manier von einem Kettenglied zum nächsten. Falls es sich um sicherheitsrelevante Prozesse handelt, kann dies zu ernsthaften Problemen führen. Die Sicherheitslogik der einzelnen AWS ist zwar stringent, jedoch können durch Seiteneinstiege Inkonsistenzen entstehen. Falls es nicht gelingt, sie zu beseitigen, scheitert die Integration. Bisher werden sicherheitslogische Inkonsistenzen nur in sehr einfach strukturierten Fällen einer Systemkoppelung oder nur innerhalb proprietärer Welten und nur mit rigiden Maßnahmen vermieden.

Seiteneinstiege sind nur bei intensiver Koppelung möglich, d.h. wenn auch Teilfunktionen verschiedener AWS gekoppelt werden können. Aber auch bei einer losen Koppelung, d.h. einer Konkatenation von ganzen Programmen ohne Auflösung in Teilfunktionen, kommt es zu Problemen, falls die AWS ihrerseits eigene dedizierte Sicherheitsfunktionalitäten enthalten.

Ziel: Sicherheitsintegration

Die herkömmliche Lösung des Problems besteht darin, ein eigenes Programm zu entwickeln, welches an der Schnittstelle zum Anwender hin als integrierendes Sicherheitstool auftritt und die einzelnen Applikationen im Durchgriff bedient. So existieren diverse Lösungen für die Großrechnerwelt, die z. B. ein *Single Sign On* ermöglichen.

Das Konzept der Sicherheitsintegration in der Mainframewelt ist hinsichtlich mehrerer Punkte erweiterungsbedürftig:

Auf der systemtechnischen Ebene muss ein Konzept zur Unterstützung von Client/Server-Architekturen und Network-Computing erarbeitet werden.

Die Konzepte sind entsprechend der neuesten Entwicklungen der Sicherheitstechnologie zu erweitern (Smartcard, Biometrie).

Es bedarf Methodiken zur Abdeckung der Sicherheit bei ablauforganisatorischen Regelungen im CSCW und Workflow Management Bereich.

Auch die Sicherheitskonzepte selbst müssen erweitert werden; z. B. neben Personenbezogenheit auch Ortsbezogenheit, Rollenbezogenheit sowie Dokumentenbezogenheit.

Security-Architektur

Das Ziel des Forschungs- und Entwicklungsprojektes ist es, begleitend zum Integrationskonzept ein adäquates Sicherheitskonzept zu entwickeln und prototypisch zu realisieren. Es ergeben sich folgende Security-spezifische Aufgaben:

- Entwicklung eines Referenzmodells einer Sicherheitsarchitektur, die auch eine intensive Koppelung von AWS ermöglicht.
- Aufbau eines Securityservers. Er muss in der Lage sein, mit anderen Securitykomponenten zu kommunizieren.

Das Server-Konzept besitzt spezifische Vorteile. Insbesondere löst der Security-Server die bei der Koppelung entstehenden sicherheitslogischen *n* zu *m* Beziehungen auf. Die damit erreichte Komplexitätsreduktion ermöglicht erst ein zuverlässiges Security Management.

forwin Lehrstuhl Prof. D. Bartmann
forwin Lehrstuhl Prof. D. Bartmann