Sicherheit im Direct Banking

Darstellung und Bewertung ausgewählter Technologien

Diplomarbeit

Andreas Kastl

Zusammenfassung

Ziel dieser Diplomarbeit ist es, ausgewählte Teilaspekte der IT-Sicherheit im Bereich des Direct Banking darzustellen und eingesetzte Technologien zu bewerten. Insbesondere die Themen Authentifizierung, Autorisierung und Single Sign-On werden näher beleuchtet, da diese als wesentliche Voraussetzung für sichere Direct Banking Anwendungen anzusehen sind. Eine Fallstudie, die bei einem führenden deutschen Finanzdienstleister durchgeführt wurde, verdeutlicht zudem die Problematik der Authentifizierung und Autorisierung und zeigt Lösungskonzepte für ein anwendungs- und plattformübergreifendes Single Sign-On auf.

Nach einem kurzen Überblick über die Grundlagen der Informationssicherheit und einer Einführung in die Kryptografie wird näher auf die Bedeutung von Authentifizierung und Autorisierung eingegangen. Dabei werden verschiedene Verfahren der Authentifizierung – wie etwa das PIN/TAN-Verfahren, zertifikatbasierende und biometrische Verfahren – sowie Konzepte der Autorisierung und Rechteverwaltung vorgestellt und bewertet.

Anschließend wird die Idee des Single Sign-On, d.h. der einmaligen Authentifizierung eines Anwenders sowie der vereinfachten Autorisierung und Administration, erläutert. Neben Vorteilen und Möglichkeiten, die ein Single Sign-On bietet, werden auch damit verbundene Gefahren und Risiken dargestellt. Zudem werden idealtypische Modelle zur Realisierung eines Single Sign-On aufgezeigt und bewertet. Beispiele für eine mögliche Realisierung von Single Sign-On bei Internet-Anwendungen und die dabei zu beachtenden Besonderheiten runden die allgemeinen Ausführungen ab.

Die darauf folgende Fallstudie beginnt mit einer Analyse der Ist-Situation des Finanzdienstleisters. Zunächst wird die IT-Architektur mit ihren verschiedenen Systemen und Anwendungen skizziert und das zugrundeliegende Authentifizierungs- und Autorisierungskonzept erläutert. Aufbauend darauf erfolgt eine Evaluation des bisherigen Ansatzes aus Sicht der Anwender und Administratoren sowie unter den Aspekten der technischen Realisierung und der Sicherheit. Hierbei werden konkrete Handlungsempfehlungen für die Verbesserung der aktuellen Situation – insbesondere unter Sicherheitsgesichtspunkten – abgeleitet.

Weiterhin werden Anforderungen an ein Sollkonzept erarbeitet und deren Realisierbarkeit durch die vorhandenen Systeme geprüft. Schließlich werden zwei Lösungskonzepte vorgestellt: eine Integrationslösung, die mit Hilfe eines Softwareagenten Single Sign-On Funktionalität bietet und die vorhandene Anwendungslandschaft weitgehend unangetastet lässt, sowie ein Neuansatz, der mit Hilfe eines zentralen Sicherheitsservices ein Single Sign-On ermöglicht, aber auch eine Anpassung der bestehenden Systeme erfordert. Die Vor- und Nachteile beider Lösungen werden abschließend ausführlich diskutiert und gegenübergestellt.

Schlüsselwörter

Sicherheit, Direct Banking, Authentifizierung, Autorisierung, Single Sign-On