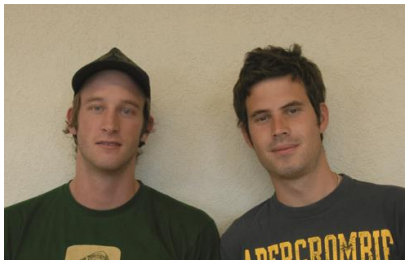
Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Transaktionssicherheit bei n-tier Anwendungen



Diplomierende
David Grunder
Florian Rettich

Dozierende
Pietro Brossi
Ewald Mund

Unternehmen, insbesondere Banken und Versicherungen, mussen seit der Einfuhrung neuer gesetzlicher Regulatorien wie dem Sarbanes-Oxley Act oder Basel II im Bereich der Transaktionssicherheit immer engere Rahmenbedingungen und Sicherheitsrichtlinien einhalten. Sie mussen dabei den Nachweis erbringen, dass ihre Transaktionen sicher sind und korrekt abgearbeitet werden.

Eine Transaktion wird definiert als Abfolge von Operationen, die nur komplett oder gar nicht, nicht aber teilweise durchgefuhrt wird. Schlagt eine Operation fehl, mussen deshalb die Daten aller beteiligten Ressourcen durch einen Rollback in den ursprunglichen Zustand gebracht werden.

Transaktionen werden in n-tier Anwendungen vorwiegend verteilt abgearbeitet. Die einzelnen Operationen konnen auf untereinander vernetzten Datenbankservern, Applikationsservern oder Back-End-Systemen erfolgen. Um die Transaktionssicherheit praventiv zu gewahrleisten, muss der Zugriff auf die in den Datentransfer involvierten Komponenten kontrolliert und beschrankt werden.

Verteilte Transaktionen in n-tier Anwendungen (Quelle: http://www.media-style.com)

Dabei durfen Transaktionen nicht isoliert betrachten werden. Es gilt, das gesamte Transaktionsumfeld zu schutzen. Dieses umfasst einerseits die IT-Umgebung (z.B. Software, verwendete Kommunikationskanale oder in Datenbanken gespeicherte Informationen der Unternehmung), andererseits aber auch den gesamten physischen Businessprozess (insbesondere den User, der die Transaktion anstosst).

Damit auch nachtraglich uberpruft werden kann, ob Missbrauche oder Security Incidents bei Transaktionen stattgefunden haben, muss ein Audit Trail definiert werden. Die Aktionen der an einer Transaktion beteiligten Knoten werden geloggt und analysiert. Durch die Analyse der Logfiles und des Audit Trails konnen sowohl unsichere Knoten, getatigte Angriffe, der Zeitpunkt der Angriffe, die Ziele der Angriffe als auch die Angreifer identifiziert werden. Dadurch konnen Schwachstellen erkannt und behoben werden.

Mit dieser Arbeit soll Revisoren ein Instrument fur den Audit von Middleware-Umgebungen in die Hand gegeben werden. Sie beschreibt die praktische Vorgehensweise und enthalt nutzliche Checklisten fur die Umsetzung.

Die Erstellung der Arbeit erfolgte in drei Phasen (Analyse, Umsetzung und