

Vertrauenswürdige Benutzer für ebensolche Services

Durchgängigen Sicherheitsrichtlinien fällt in serviceorientierten Architekturen eine wichtige Rolle zu. Allerdings sollten diese nicht nur auf dem Papier definiert sein, um Wirkung zu zeigen.

WIEN – Serviceorientierte Architekturen stellen hohe Anforderungen an die Sicherheit. Derartige Probleme können mit so genannten *Trust Zones* gelöst werden; in deren Rahmen werden vertrauenswürdige Services und Benutzer definiert, wodurch Sicherheitsstandards zentral auf Prozessebene sichergestellt werden könnten, wie Eric Schaumlöffel, seines Zeichens Senior Technology Consultant bei

Progress Software, erklärt. »Mit einer serviceorientierten Architektur können Unternehmen Applikationen aus einer wachsenden Anzahl interner und externer Services zusammenstellen, die in einer föderativen Infrastruktur verteilt sind.« Doch die Wiederverwendung und gemeinsame Nutzung dieser Services stelle eine große Herausforderung für die Sicherheit der Anwendungen dar. »Sicherheitsaspekte

können sogar zu einem entscheidenden Faktor für den Erfolg einer SOA werden.«

RICHTLINIEN NICHT NUR AUF PAPIER DEFINIEREN

Die lose Kopplung von Services zählt zu den Merkmalen einer SOA. Obwohl die Kommunikation zwischen Services durch einen Enterprise Service Bus gesichert werden könne, müssten auch die Services selbst gesichert werden. »Insbesondere wenn sie sich außerhalb des Busses befinden und etwa durch Webservices aufgerufen werden.« Die Definition vertrauenswürdiger Services und Benutzer – so genanntes *Trust Zoning* – könne beispielsweise über eine Richtlinie umgesetzt werden, mittels derer festgelegt wird, dass ein

bestimmter Service nur von bestimmten Nutzern oder nur über ein bestimmtes Gateway aufgerufen werden darf. »Das unvermeidliche Sicherheitsproblem einer SOA lässt sich beispielsweise durch eine Technologie wie Progress Actional lösen, mit der eine Definition vertrauenswürdiger Zonen erfolgen kann.« Dabei werde eine kompakte Policy Engine Proxy verwendet, die sich zwischen einem Service und dessen Konsument befinde. »Gesteuert wird diese über ein zentrales Bedienungsfeld, das nicht nur zentrale Erstellung, Konfiguration und Implementierung von Richtlinien auf verteilten Proxys, sondern gleichzeitig auch die Sammlung detaillierter Datenfluss- und Interaktionsinformationen zur IT-Betriebsumgebung er-

möglicht.« Auf dieser Basis könnten Nutzer Regeln definieren, mit denen unterschiedlichste Anforderungen und Funktionen von Services beschrieben werden.

So könnte ein Unternehmen beispielsweise eine Richtlinie für eine Sicherheitsanforderung definieren, mit der festgelegt wird, dass ein bestimmter Service nur von bestimmten Benutzern des jeweiligen Standorts aufgerufen werden darf. »Anstatt Richtlinien nur auf dem Papier festzulegen – was generell fehleranfällig ist und im Falle von Änderungen auch einen hohen Zeitaufwand mit sich bringt – sorgt eine Proxy Engine dafür, dass die Einhaltung von Richtlinien zur Laufzeit und im Kontext der Interaktion überprüft und sicher gestellt wird.« [tn]

Der Enterprise Service Bus sorgt in einer SOA für eine transparente Infrastruktur und bildet damit eine wichtige Voraussetzung für effizientes Management.