

Statement of the Month – Novell Consulting

Düsseldorf im März 2007

SOA – zwischen größerem Bewegungsspielraum und stringenterem Regelwerk

SOA steht ganz im Zeichen der Serviceorientierung, in einer SOA gibt es daher eigentlich keine Anwendungen mehr, sondern nur noch Services. Diese werden dem Anwender mit offenen Schnittstellen „lose“ über eine zentrale Integrationsplattform zur Verfügung gestellt. Wenn zum Beispiel eine Fachabteilung ein neues Tool anfordert, dann wurde früher häufig dafür in einem Einzelprojekt eine entsprechende solitäre Anwendung erstellt, die die gewünschten Funktionen aufwies. Im Rahmen einer SOA wird die angeforderte Funktion heute als Service über eine zentrale Infrastruktur angeboten. Eine SOA hat daher den Vorteil, dass Services (also die Anwendungen bzw. Ressourcen) bei Bedarf auch anderen Anwendern des Unternehmens oder Partnern zugänglich gemacht und mit anderen Anwendungen – etwa Datenbanken, System- und Speichermanagement, SAP – in Form von Prozessketten verknüpft werden können. Durch diese Bauweise können die IT-Ressourcen also vielseitiger und flexibler genutzt werden, was Effizienzvorteile mit sich bringt und schnelles Reagieren am Markt erst möglich macht.

So die Theorie. In der Praxis werfen sich hier aber einige Fragen auf, vor allem, was die Verwaltung oder die Autorisierung und Authentifizierung der Nutzer betrifft: Wenn die Anwendungen ineinandergreifen sollen – wie funktioniert das dann mit den unterschiedlichen Zugriffsrechten je Anwendung? Wie lässt sich eine solche Infrastruktur überhaupt sicher gestalten? Hier geht es unter anderem um den zentralen Konflikt zwischen dem Bedarf nach schneller Reaktionsbereitschaft am Markt durch die schnelle Bereitstellung von IT-Ressourcen und dem Bedarf nach sicherem Zugang zu den Ressourcen und der Zeit, die man für diese Sicherheit aufbieten muss. Mit anderen Worten: Um die größere Freiheit und Beweglichkeit einer SOA zu nutzen, braucht es feste Regeln. Die oben gestellten Fragen sowie diejenigen nach Qualitätssicherung, Verfügbarkeit, Komponentenwechsel, Performance und Zuverlässigkeit müssen also im Rahmen einer SOA Governance beantwortet werden. Andernfalls droht das Chaos, denn eine SOA verfügt über zu viele bewegliche Einzelteile, die kreuz und quer im Unternehmen eingesetzt werden und die ohne festes Regelwerk aus dem Ruder laufen können. Davon hat niemand etwas und eine SOA droht aufgrund ihrer zu großen Beweglichkeit an Leistungsvermögen und Effizienz einzubüßen.

Essentieller Bestandteil dieser SOA Governance muss das Identitäts- und Zugangsmanagement

sein. Denn sicher ist, dass im Rahmen einer SOA-Struktur das Zugangsmanagement schlecht mit den verschiedenartigen, mit den Anwendungen mitgelieferten Zugangssystemen geleistet werden kann. Diese sind lediglich eine Art Blackbox, die sich nur schwer in die Offene-Standards-Strategie einer SOA integrieren lassen. Eine SOA ist nicht reaktionsfähig, wenn sich der Nutzer bei jedem einzelnen Service erst anmelden muss. Geschweige denn, dass man unter diesen Umständen jeden Zugriff ordnungs- und vor allem Compliance-gemäß jederzeit nachweisen kann. Und das Problem betrifft nicht nur die Anwendungsebene, sondern vor allem auch die Datenebene – hier ist es sogar ungleich komplizierter, Inhalte konsistent vor unbefugten Einblicken zu schützen. Dies zeigt deutlich, dass eine SOA nur mit einer umfassenden Identity- und Access-Management-Strategie und -Lösung funktionieren kann. Die IAM-Hersteller haben sich mittlerweile auf den SOA-Einsatz vorbereitet, indem sie der Software möglichst viele Schnittstellen mitgeben und allgemein auf offene Standards bauen.

Viele Schnittstellen und die Organisation unterschiedlicher Anwendungen, die miteinander in Beziehung stehen, bringen zudem die Gefahr mit sich, den Zusammenhang von Ereignissen innerhalb einer SOA-Infrastruktur aus dem Blick zu verlieren. Abhilfe kann da ein zentrales "Security Information and Event Monitoring" (SIEM)-Tool schaffen, das auf Basis vordefinierter Regeln Informationen und Events aus allen Ressourcen im Unternehmensnetzwerk sammelt, diese Daten normalisiert, korreliert, aggregiert und direkt Aktionen zur Behebung auslöst - entweder manuell oder teil- und vollautomatisiert. Sämtliche Vorgänge werden dabei dokumentiert, über ein Dashboard transparent gemacht und in einer zentralen Datenbank gespeichert, so dass diese auch im Nachgang (Audit) noch nachvollzogen werden können, zum Beispiel bei Änderungen der Zugriffsberechtigungen oder der Prozesse innerhalb der SOA. Bei Regelverstößen wird ein Alarm ausgelöst und je nach Relevanz ein Behebungsprozess angestoßen. Und da alles nahtlos dokumentiert ist, lassen sich mittels Analysen systemisch Schwachstellen beheben.

SOA und IAM sind weit davon entfernt, sich im Rahmen einer SOA-Governance gegenseitig auszuschließen. Das zeigt auch die Tatsache, dass ein unternehmensweites Single-Sign-On-System auf Basis von Identity und Access Management-Anwendungen einer der wichtigsten SOA-Services und häufig eine der ersten Anwendungen überhaupt ist, die ein Unternehmen SOA-mäßig aufbereitet. Insofern herrscht zwischen SOA Governance und IAM weniger eine Zwangsheirat, als eine Liebesheirat.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der

führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachusetts (USA), beschäftigt weltweit rund 4.700 Mitarbeiter. Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter www.novell.com oder www.novell.de.

Pressekontakt:

Dorothee Stommel

Text 100 Public Relations

Tel: ++49 - (0)89 - 99 83 70-89

E-Mail: novell@text100.de

Ihre Ansprechpartnerin bei Novell:

Ulrike Beringer

PR Manager Novell Central Europe

Tel: ++49 - (0)89 - 206002118

E-Mail: uberinger@novell.com