www.bt-magazin.de 1.10

Deutschland: € 14,90 Österreich: € 16,80 Schweiz: sFr 29,80 Luxemburg: € 16,90

Business Technology

Business Technology

Architektur & Management Magazin

Expertenwissen für IT-Architekten, Projektleiter und Berater

Erl:
„SOA in a Box hat die Probleme verursacht"

Schwerpunkt:
Software Architektur

Businessorientierte Architekturansätze

Kanban in Softwareprojekten

Pragmatic SOA – Beschränken auf das Wesentliche

Servicesichten
Den passenden Service finden

People Change Management
Änderungsprozesse erfolgreich meistern

How does IT matter?
Den Wertbeitrag der IT bestimmen

Enterprise SOA Security
Teil 1: Die Herausforderungen

Aus alt mach neu
Die 10 Regeln der Modernisierung

4 191858 414906 01

Enterprise SOA Security

Herausforderungen Teil 1

AUTOREN: DR. DIRK KRAFZIG, JOST BECKER,
OLIVER MAHNKE, ILJA PAVKOVIC

Der nachhaltige Nutzen serviceorientierter Architekturen (SOA) ist nach dem großen Hype von 2006 und 2007 und der darauf folgenden Findungsphase heute allgemein anerkannt. Nahezu jedes Unternehmen befasst sich mit SOA, und Neuprojekte berücksichtigen wie selbstverständlich die zugrunde liegenden Prinzipien. Damit werden sich über die nächsten Jahre die Spielregeln, nach denen Unternehmens-IT funktioniert, auf grundlegende Weise ändern. An die Stelle traditioneller, weitgehend isolierter Siloanwendungen werden fachlich ausgerichtete Services treten, die über Abteilungs- und Unternehmensgrenzen hinweg zur Unterstützung umfassender Geschäftsprozesse miteinander verknüpft werden können. Aus den Silos werden Funktionen extrahiert und als wiederverwendbare Services einem breiten Nutzerkreis bereitgestellt. Eine damit einhergehende stärkere Ausrichtung der IT am Geschäft wird zu einer deutlichen Steigerung des Wertbeitrags sowie der Produktivität der IT führen. SOA wird Unternehmen erlauben, ihre Geschäftsprozesse und Organisationsstrukturen in dynamischen Märkten flexibel den wechselnden Gegebenheiten anzupassen.

Vierteilige Reihe: Enterprise SOA Security

Teil 1: Herausforderungen
Der erste Teil befasst sich mit den Herausforderungen heutiger IT-Landschaften. Abteilungsübergreifende, integrierte Lösungen und die Öffnung von Kernsystemen für Kunden und Lieferanten überfordern häufig traditionelle Sicherheitslösungen

Teil 2: Lösungsmuster
Im zweiten Teil der Serie werden Lösungsmuster vorgestellt, mit deren Hilfe moderne SOA Security konzipiert werden kann. Im Zentrum der Diskussion stehen Security-Token, die in einer verteilten Umgebung sicherstellen, dass jede Komponente gesicherte Annahmen über ihre Nutzer und deren Berechtigungsprofile treffen kann

Teil 3: Web-Services-Standards
Zahlreiche Web-Services-Standards wie SAML, WS-Security, XACML oder WS-Trust helfen bei der Umsetzung interoperabler Sicherheitslösungen in einer SOA. Der dritte Teil gibt einen Überblick über existierende Standards und wie sie in der Praxis angewandt werden

Teil 4: Organisatorische Maßnahmen
SOA Security ist keinesfalls ein reines Technologiethema. Abteilungsübergreifende Prozess- und Rollenkonzepte erfordern auch abteilungsübergreifende Governance und ein Umdenken in den Risikoabteilungen großer Unternehmen.

WARUM BRAUCHT SOA EIGENE SECURITY-KONZEPTE?

Es ist heute allgemein anerkannt, dass die Transformation traditioneller IT-Landschaften hin zu SOA ein langjähriger Prozess ist, der auf verschiedenen organisatorischen und technischen Ebenen wirken muss. Dieser Artikel befasst sich mit einer dieser Ebenen – der Security, ohne die jede SOA-Initiative früher oder später ins Stocken geraten wird. Dabei ist es gar nicht verwunderlich, dass traditionelle Security-Lösungen nicht eins zu eins in die SOA-Welt übertragen werden können. Neue Konzepte sind nötig, da traditionelle und serviceorientierte IT-Landschaften zum Teil sehr unterschiedliche Anforderungen an die Sicherheit haben (Tabelle 1).

Wenn sich ein Unternehmen für die Einführung einer SOA entschieden hat, müssen aus oben genannten Gründen so früh wie möglich die richtigen Securityme-

chanismen etabliert werden: Dabei geht es um nichts weniger, als das grundlegende Verständnis von Security zu erneuern. In der Vergangenheit wurde Security häufig auf der Ebene einzelner Anwendungen betrachtet. Konzepte und Technologien wurden auf die Bedürfnisse der jeweiligen Anwendung abgestimmt. Dies ist in einer SOA nun nicht mehr möglich. In einer SOA ist Security eine Angelegenheit, die auf Unternehmensebene gelöst werden muss.

Betrachten wir dazu ein kleines Beispielszenario: Ein Produktionsunternehmen nutzt für seine Produktion Maschinen und benötigt Software, die verschiedene Geschäftsvorfälle im Zusammenhang mit diesen Maschinen unterstützt – z. B. die Anschaffung, den operativen Betrieb und die Wartung. In einer SOA stellt man zentral verfügbare Services bereit, die die Daten zu diesen Maschinen verwalten. Diese Services werden über entsprechende Anwendungssysteme durch Mitarbeiter aus unterschiedlichen Abteilungen genutzt – z. B. Einkäufer, Produktionsmitarbeiter und Wartungstechniker. Jede Benutzergruppe (oder auch Rolle) hat dabei unterschiedliche Berechtigungen, Maschinendaten zu lesen und zu ändern.

Dabei ist es nicht nur die Funktionalität rund um das fachliche Geschäftsobjekt *Maschine*, die in einem unternehmensweit gültigen Service eingepackt wird. Auch die Berechtigungsregeln, die den Zugriff auf Maschinendaten steuern, müssen auf Unternehmensebene definiert werden. Folgerichtig stehen Sie vor der Aufgabe, unternehmensweit Rollen und deren Berechtigungen abzustimmen. Mit traditioneller Security werden Sie in einer SOA aber schnell auf Schwierigkeiten stoßen, diese unternehmensweite Sichtweise herzustellen. Traditionelle Security bietet weder die organisatorischen Strukturen und Prozesse noch die Technologien, die Sie in der Verwaltung unternehmensweiter Rollen und Berechtigungsregeln unterstützen. Nicht ohne Grund betrachten laut einer Studie von GMG Insights aus dem Jahr 2008 [1] weltweit 43 % der befragten IT-Verantwortlichen Securityüberlegungen als den kritischsten Punkt bei der Implementierung von SOA-/Web-Service-Anwendungen. Schauen wir nun etwas tiefer ins Detail. Wenn Sie sich bereits mit Securityaspekten in traditionellen IT-Landschaften beschäftigt haben, werden Ihnen einige der folgenden SOA-Anti-Pattern bekannt vorkommen.

	Traditionelle Security	Enterprise SOA Security
Unternehmens-architektur	Weitgehend isolierte Anwendungssilos, Datenaustausch zwischen Silos mit EAI	Übergreifende Geschäftsprozesse, Querschnittsfunktionalität in SOA-Services ausgelagert
Scope einer Security-Lösung	Einzelne Anwendungen oder Datenbanken	Geschäftsbereich, Firma oder sogar firmenübergreifende Lieferkette
Technologie	Proprietäre Betriebssystem- und Datenbanksecuritymechanismen	Offene Standards wie WS-Security, SAML, XACML etc.
Administration	Beantragung von Rechten auf Unternehmensebene,konkrete Umsetzung auf Abteilungsebene. In der Praxis findet man auch viele Ausnahmen und Sonderregeln, die die zentrale Kontrolle aushebeln	Administration in der Regel auf Bereichsebene. Dabei werden z. B. Rollenkonzepte der unterschiedlichen Bereiche miteinander abgestimmt
Kontrolle durch Fachbereiche	Hoch Fachbereich ist Owner seines Systems und hat direkten Durchgriff auf Securitykonfiguration	Gering Security liegt außerhalb der Verantwortung der Fachsysteme, damit schwindet deren Kontrolle
Einmalkosten	Keine	Kosten durch Initialprojekt zum Aufsetzen der Enterprise SOA Security
Laufende Kosten	Versteckt in den einzelnen Anwendungen. Fehlende Transparenz auf Unternehmensebene	Überwiegend zentral, dadurch nachvollziehbar Ab einer kritischen Größe der IT-Landschaft geringer als die traditioneller Security
Berechtigungsmodell	Typischerweise Owner- oder ressourcenorientiert	Claim-/Rollenbasiert
Single Sign-on	Schwierig und teuer	Einfach, nur geringe Zusatzkosten
Anbindung von Kunden und Lieferanten	Schwierig und teuer In der Regel wird auf hohe Sicherheitsstandards verzichtet	Einfach, nur geringe Zusatzkosten
Grad der Standardisierung	Mittel bis gering	Hoch
Unterstützung von Compliance-Vorhaben	Schlecht Compliance muss Anwendung für Anwendung individuell betrachtet werden	Gut Einheitliche Konzepte erleichtern Verständnis der Unternehmens-IT

Tabelle 1: Gegenüberstellung der Security in traditionellen und serviceorientierten IT-Landschaften

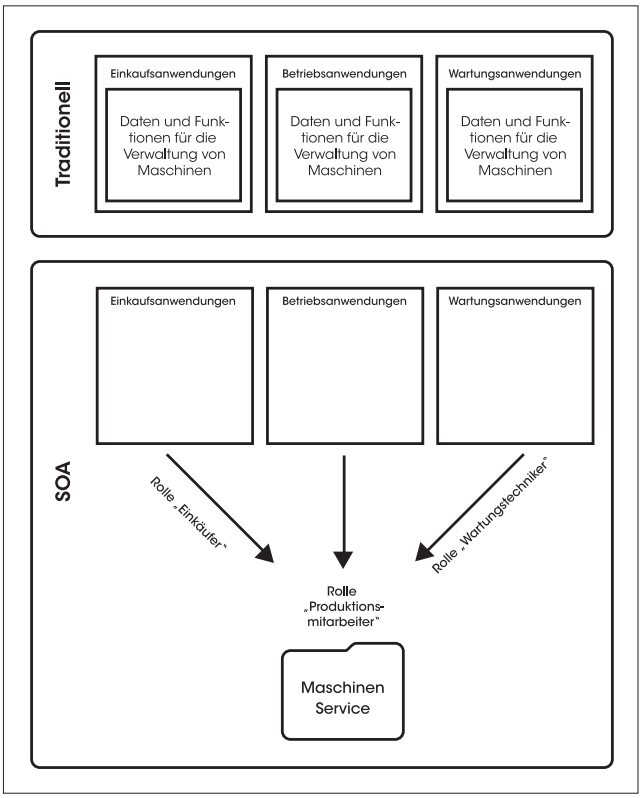

Abb. 1: Enterprise SOA Security erlaubt es verschiedenen Anwenderrollen, aus unterschiedlichen Abteilungen geregelt auf zentralisierte Services zuzugreifen

Kenntnis der Identität des Nutzers wird vorausgesetzt: Unabhängig davon, ob Rollen und Rechte dezentral in den Anwendungen oder zentral verwaltet werden, wird in heutigen IT-Landschaften praktisch immer die Kenntnis der Identität der Nutzer vorausgesetzt. Während eine dezentrale Lösung aufgrund von redundantem Identitätsmanagement und multiplen Sign-on-Vorgängen ohnehin viele Nachteile hat, erlaubt eine zentrale ID-Verwaltung immerhin das zentrale Anlegen und im Bedarfsfall auch Deaktivieren von Nutzern. Beide Ansätze haben gemein, dass der Nutzer vor einer Vergabe von Rollen/Rechten im betreffenden System angelegt und während des laufenden Betriebs verwaltet werden muss. Ein derartiges Verfahren schränkt das Anbieten oder das Nutzen von Services (ggf. auch externen Services) erheblich ein.

Identitäten und Rechte sind eng gekoppelt: Benutzeridentitäten und die dazugehörigen Rechte werden in einem gemeinsamen System verwaltet und sind untrennbar (oder nur sehr schwer trennbar) miteinander verquickt.

Rechte werden Individuen zugeordnet: Die direkte Vergabe von Rechten an einzelne Personen statt an Rollen ist auch in traditionellen IT-Architekturen problematisch. Der Zugriff auf IT-Funktionalität darf in keinem Unternehmen von der Existenz eines Individuums abhängig sein.

Rechte werden von ungeeigneten Eigenschaften abgeleitet: Es ist gängige Praxis und absolut korrekt, dass eine Abteilungszugehörigkeit einem Mitarbeiter einen definierten Satz Rechte sichert. Werden Rechte aber beispielsweise über den Abteilungsnamen vergeben, führt jede Umstrukturierung des Unternehmens mindestens temporär zum Kollaps bzw. zu erheblichem – und dabei eigentlich völlig überflüssigem – Anpassungsaufwand.

Keine Berechtigungsprüfung bei gegenseitigen Systemaufrufen: Innerhalb einer geschlossenen Systemlandschaft wird einer aufrufenden Anwendung häufig blind vertraut. Allein die Kenntnis und die korrekte Bedienung nicht öffentlicher Schnittstellen wird als Autorisierung akzeptiert. Dies stellt ein unnötiges Sicherheitsrisiko dar.

Abteilungsindividuelle Autorisierungsregeln: In den seltensten Fällen sind die notwendigen Autorisierungsregeln über Abteilungsgrenzen hinweg abgestimmt, d. h. selbst die Vorgaben unterscheiden sich von Abteilung zu Abteilung in Form und Inhalt.

Anwendungsindividuelle Implementierung, Administration und Betrieb von Securitykomponenten: Wenn bereits die Vorgaben nicht abteilungsübergreifend abgestimmt sind, ist es von den konkreten Implementierungen ebenfalls nicht zu erwarten. Tatsächlich ist die Realisierung unterschiedlichster Securitykonzepte mit stark variierenden Detaillösungen Realität in Unternehmen jeglicher Größe – inklusive der dadurch für jede Abteilung zu tragenden Kosten für mehrfache Planung, Implementierung und Betrieb.

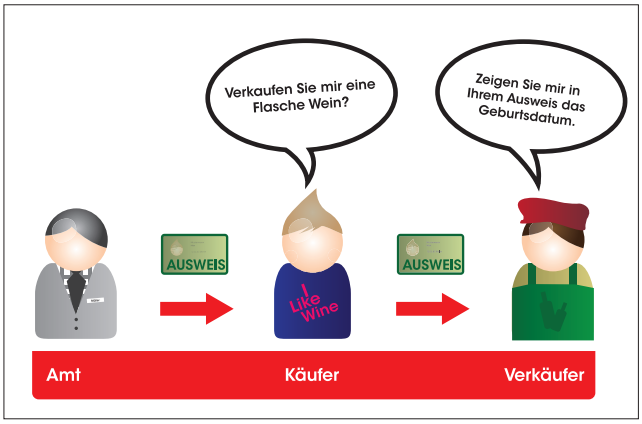

Abb. 2: Enterprise SOA Security basiert zur Autorisierung auf Security Token und nicht auf Benutzeridentitäten. Vereinfacht dargestellt, halten Security Token gesicherte Informationen über Nutzer und ihre Eigenschaften

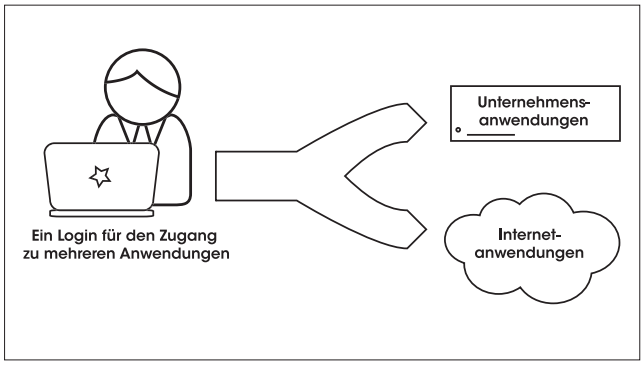

Abb. 3: Verkauf von Wein ist nur Erwachsenen ab 16 gestattet

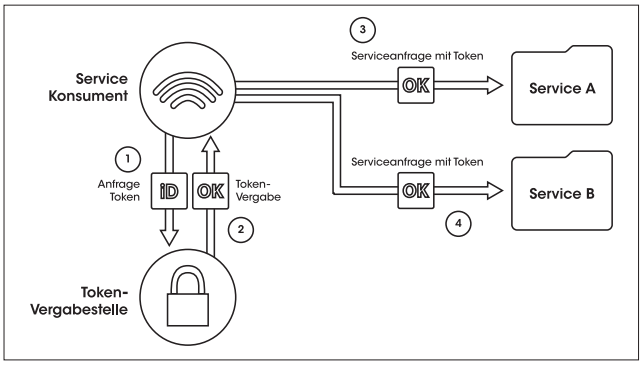

Abb. 4: Vorteile von Enterprise SOA Security

Die beschriebenen Problemfelder verdeutlichen, dass der Versuch, traditionelle Verfahren in einem offenen, verteilten System anzuwenden, zum Scheitern verurteilt ist. Bereits die Anforderung, die Identität des Konsumenten zu kennen, kann ein Projekt vor unlösbare Probleme stellen. Und dabei geht es – beispielsweise bei Autorisierungen – in den seltensten Fällen um die Überprüfung einer exakten Identität, also der vollständigen Menge aller Identitätsmerkmale, sondern vielmehr um eine situationsbedingte Bestätigung einzelner Merkmale eines Nutzers. Eine kleine Analogie soll dies verdeutlichen: Für den Erwerb einer Flasche Wein ist es irrelevant, ob Sie männlichen oder weiblichen Geschlechts sind, wo Sie wohnen oder wie Ihr vollständiger Name lautet. Einzig die Tatsache, ob Sie das 16. Lebensjahr vollendet haben, entscheidet darüber, ob Sie konsumieren dürfen oder eben nicht. Im täglichen Leben genügt eine Altersbestätigung in Form eines Personalausweises, ausgestellt durch eine dritte, vertrauenswürdige Instanz, dem zuständigen Meldeamt. Eine Vorgehensweise, die wir uns merken sollten ...

SECURITY IST KEIN HOBBY ...

Die Wenigsten beschäftigen sich aus purer Freude mit IT-Sicherheit. Aufgrund der Vielfältigkeit der Thematik muss Security diszipliniert, verantwortungsvoll und mit zentraler Bedeutung umgesetzt werden.

... SONDERN VIELMEHR EXISTENZSICHERUNG

Die Notwendigkeit, sich mit Security intensiv auseinanderzusetzen, ergibt sich vielmehr aus Zwängen. Dem Zwang, den Wissensvorsprung des eigenen Unternehmens vor dem Wettbewerb zu bewahren, dem Zwang, mit schützenswerten Daten wie z. B. Personal- oder Krankenakten verantwortungsbewusst umzugehen, dem Zwang, historisierte Datenbestände konsistent und abrufbar zu halten, um gesetzlichen bzw. Revisionsvorgaben gerecht zu werden etc. Für bestimmte Rechtsformen existieren gesetzliche Regelungen wie der Sarbanes-Oxley Act (SOX) oder das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), deren Kernforderung nach Korrektheit und Belastbarkeit der veröffentlichten Finanzdaten von Unternehmen ein existierendes und sicher funktionierendes Risikomanagementsystem bedingt. Neben ausgeweiteten Haftungsgrundlagen für das erweiterte Management – Vorstände, Aufsichtsräte, Wirtschaftsprüfer und sogar Projektleiter – nehmen derartige Vorgaben und ihre Umsetzungen im Rahmen von Ratings wie Basel II auch indirekten Einfluss auf wirtschaftliche Erfolgsfaktoren der Unternehmen.

WAS KANN ENTERPRISE SOA SECURITY LEISTEN?

Bereits heute stehen viele Lösungsbausteine zur Umsetzung der Sicherheitsanforderungen serviceorientierter Architekturen bereit. Diese bieten gleichzeitig eine Menge weiterer Vorteile.

Offene Standards: Es existieren offene Standards, auf denen Sie Ihre Enterprise SOA Security aufbauen

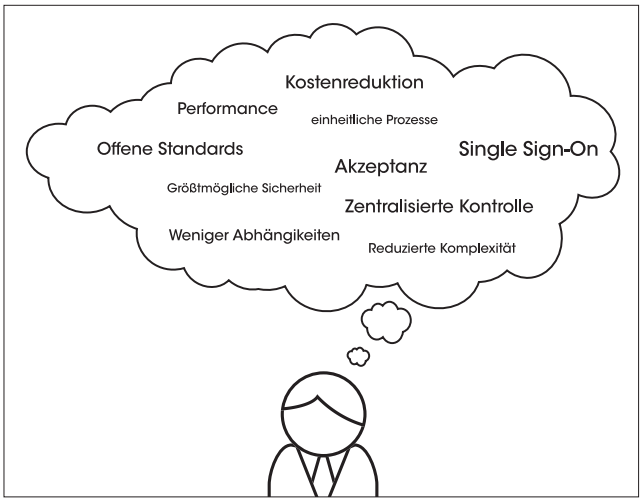

Abb. 5: Single Sign-on (SSO)

können. Alle Vorteile offener Standards wie Interoperabilität, Unabhängigkeit, Verfügbarkeit von Beratern u. v. m. gelten auch hier [3].

Einheitliche Prozesse: Mit der Einführung von Enterprise SOA Security geht in der Regel die Standardisierung zahlreicher IT-Prozesse einher. Diese Standardisierung stellt einen Wert an sich dar. Die erzwungene projektübergreifende Umsetzung der Securityanforderungen verhindert individuelle Interpretationen der Sicherheitserfordernisse, die zu individuellen Lösungsversuchen einer bereits gelösten Problematik führen.

Zentralisierte Kontrolle: Der positive Einfluss einer übergeordneten Security-Governance erstreckt sich über die Entwicklungsphasen bis in den Betrieb. Beispielsweise können Nutzer zentral und redundanzfrei angelegt, aktiviert, bezüglich ihrer Rollen und Rechte angepasst und ggf. gesperrt werden.

Reduzierte Komplexität, weniger Abhängigkeiten: Standardisierte SOA-Security-Mechanismen sind leicht zu verstehen und reduzieren den Aufwand in Projekten spürbar, da diese auf eine vorhandene und eingespielte Infrastruktur zurückgreifen können.

Kostenreduktion: Die Vermeidung redundanter Insellösungen garantiert, dass Ihre standardisierte SOA-Security-Implementierung signifikante Einsparungen während des Betriebs realisiert. Zusätzlich spart die Wiederverwendung von technischer Querschnittsfunktionalität auch Kosten in der Testphase jedes Fachprojekts.

Single Sign-on: Die Notwendigkeit, sich mehrmalig anzumelden, ist nicht nur für den Nutzer eine unangenehme Tätigkeit, sondern auch eine Produktivitätsbremse und ein Sicherheitsrisiko. Mit SOA Security können Sie ohne großen Mehraufwand auch Single-Sign-on-(SSO-)Lösungen realisieren.

Performance: Ein standardisiertes Securityrahmenwerk, das zentral bereitgestellt wird, kann auch zentral optimiert werden. Dies bietet die Möglichkeit, auch in die Optimierung von Performanceaspekten zu investieren. Einzelne Fachprojekte haben hierfür in der Regel kein Budget und verzichten im Zweifelsfall eher auf Sicherheit.

Größtmögliche Sicherheit: Resultat der vorgestellten positiven Aspekte ist in Summe die maximale Sicherheit, die Sie heute in verteilten Anwendungslandschaften erreichen können.

Akzeptanz: Last but not least erreichen Sie mit Enterprise SOA Security das höchste Maß an Akzeptanz für Security in Ihrem Unternehmen.

ZUSAMMENFASSUNG UND AUSBLICK

Wir hoffen, mit diesem Artikel Ihr Bewusstsein für die unabdingbare Notwendigkeit geweckt zu haben, sich intensiv mit den geänderten Anforderungen an Security in verteilten Systemen auseinanderzusetzen. SOA Security hilft Ihrem Unternehmen, sich in einem dynamischen Marktumfeld zu behaupten. Ihnen persönlich hilft SOA Security, sichere Projektlösungen zu schaffen, ohne das Rad jedes Mal neu erfinden zu müssen. Enterprise SOA Security ist alternativlos, wollen Sie nicht mit veralteten Konzepten an aktuellen Herausforderungen scheitern, wie es gerade in der jüngsten Vergangenheit auch namhafte Großunternehmen demonstriert haben.

Nachdem wir in diesem Artikel gezeigt haben, welche Herausforderungen zu bewältigen sind und welche Vorteile eine adäquate Securitystrategie bietet, werden sich die folgenden Artikel dieser kleinen Reihe dem Wie widmen. Sollten Sie also in Ihrem Unternehmen vor der Aufgabe stehen, eine Enterprise-SOA-Strategie zu entwickeln, können Sie noch heute mit dem Entwurf der Security beginnen. Ein zu früh gibt es dafür nicht.

Dr. Dirk Krafzig ist Gründer von SOAPARK. Als Sprecher auf Konferenzen und Autor von Artikeln und Büchern gilt Dr. Krafzig als ein Protagonist der serviceorientierten Architektur (SOA) und hat maßgeblich zu der Begriffsbildung in diesem Bereich beigetragen. Insbesondere die SOA-Fallstudien mit Deutscher Post, Credit Suisse, Halifax Bank of Scotland und Winterthur Versicherung in seinem Bestseller „Enterprise SOA, Prentice Hall, 2004." haben viel Aufmerksamkeit auf sich gezogen. Derzeit arbeitet Dr. Krafzig in einem strategischen SOA-Programm bei einem Mobilfunkanbieter an dem Thema Security.

Jost Becker ist gemeinsam mit Ilja Pavkovic und Oliver Mahnke Gründer der binaere bauten gmbh. Sein Interesse gilt parallel zu informationstechnologischen Themen seit jeher ökonomischen und organisatorischen Aspekten im Unternehmen – eine Kombination, die sich in seinem aktuellen Tätigkeitsfeld als Berater für Software- und IT-Unternehmensarchitekturen auszahlt. Aktuell richtet er seinen Fokus auf die speziellen Securityanforderungen in verteilten Systemen.

Oliver Mahnke ist Chefarchitekt der binaere bauten gmbh. In dieser Rolle verantwortet er sowohl Anwendungs- als auch Unternehmensarchitekturen. Derzeit erarbeitet er die zentralen Architekturrichtlinien für eines der größten deutschen Versicherungsunternehmen.

Ilja Pavkovic hat langjährige praktische Erfahrung in strategischen und global aufgestellten IT- Projekten. In wechselnden Rollen als Projektleiter und Softwarearchitekt bildeten generative Softwareentwicklung und Security immer wieder Schwerpunkte. Insbesondere kennt er auch traditionelle Securitylösungen – und ihre Grenzen.

Links & Literatur

[1] Global Report on SOA/Web Services Security Initiatives, GMG Insights, September 2008

[2] Bundesamt für Sicherheit in der Informationstechnik: SOA-Security-Kompendium, Version 2.0, 2009

[3] Dabei liegt es in der Natur der Sache, dass Sie die von Ihnen zur Verwendung vorgesehenen Standards sorgfältig auswählen müssen, um Redundanzen oder mögliche Konflikte zu vermeiden.