www.bt-magazin.de 1.2011 Heft 4 Deutschland: € 14,90 Österreich: € 16,80 Schweiz: sFr 29,80 Luxemburg: € 16,90

Business Technology

Business Technology

Architektur & Management Magazin

Krause:
„Integration führt zu Koexistenz."

Expertenwissen für IT-Architekten, Projektleiter und Berater

Schwerpunkt:

INTEGRATION

Über die Marke zum Erfolg
Integrationslösungen dauerhaft etablieren

Softwareprojekte über Unternehmensgrenzen hinweg
Benötigen wir neue Organisationsformen zur Integration von Spezialisten?

Trari, Trara, die Post ist da!
Der Servicebus in der Cloud

Informationszentrische Softwareintegration
Agilität und Flexibilität durch eine Referenzarchitektur

Enterprise SOA Security
Teil 4: Organisatorische Maßnahmen

Evolution der Integrationsarchitektur

Integrationsprozesse innovativ inszeniert

Integration aus der Schachtel

4 191858 414906 01

Organisatorische Maßnahmen, Teil 4

Enterprise SOA Security

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

Die Auslagerung von Querschnittsfunktionalität in Services sowie die automatisierte Ausführung unternehmensweiter Geschäftsprozesse stellen neue Herausforderungen dar, die durch die Securitykonzepte traditioneller Silo-Lösungen nicht angemessen realisierbar sind. So ist Security zukünftig transparent, rollenbasiert, unternehmensweit einheitlich und standardisiert umzusetzen, um auf Unternehmensebene beispielsweise die geforderte Transparenz und Kontrolle zu schaffen. Der vierte und letzte Teil unserer SOA-Security-Reihe beschäftigt sich abschließend mit der organisatorischen Blaupause zur konkreten Umsetzung von Enterprise SOA Security.

STRATEGISCHE ASPEKTE

In der Anfangseuphorie von SOA wurde dem Thema Security wenig Aufmerksamkeit geschenkt. Andere Themen, insbesondere die Einführung von ESBs und Repositories sowie die Strategieentwicklung standen im Vordergrund. Durch die steigende Verbreitung von Web Services und der damit verbundenen Öffnung bisheriger Silo-Anwendungen stellt sich jetzt die Herausforderung, auch das Thema Security als Teil der SOA-Strategie zu etablieren.

Der erste Schritt hierfür ist die Analyse möglicher Angriffsszenarien und der damit verbundenen Risiken. Ohne dieses elementare Verständnis besteht die Gefahr, Investitionen in Security fehlzuleiten. Jede Organisation muss dabei eine individuelle Risikobewertung vornehmen. Diese ist die Grundlage eines Fahrplans zur Implementierung von Enterprise SOA Security, der die individuelle Risikolage ihres Unternehmens auch tatsächlich angemessen adressiert. Betrachtet man beispielsweise ein Bankhaus, so ist der Schaden sehr hoch, der im Fall nicht oder nur fehlerhaft durchgeführter Transaktionen entstehen kann. Die Kernkompetenz der geschädigten Bank wird in Frage gestellt und die Hauptverdienstquelle gerät in Gefahr. Gepaart mit einer hohen Eintrittswahrscheinlichkeit, ist das Risiko korrupter Transaktionen folglich als hoch zu bewerten. Betrachtet man dagegen die Anbindung von

Vierteilige Reihe: Enterprise SOA Security

Teil 1: Herausforderungen Erschienen in Ausgabe BT 1.10	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 Erschienen in Ausgabe BT 2.10	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 Erschienen in Ausgabe BT 3.10	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 Vorliegende Ausgabe	SOA Security ist keinesfalls ein reines Technologiethema. Abteilungsübergreifende Prozess- und Rollenkonzepte erfordern auch abteilungsübergreifende Governance und ein Umdenken in den Risikoabteilungen großer Unternehmen.

Vertriebspartnern, könnte die Risikobewertung anders ausfallen und zu anderen Prioritäten führen. Beispiele für strategisch relevante Sicherheitsaspekte sind Folgende:

- *Schutz vor korrupten Geschäftstransaktionen*: Fehlgeleitete Geld- und Warenflüsse bzw. entstehender Aufwand zur Verfolgung und Korrektur stellen hier die größten finanziellen Risiken dar
- *Schutz geheimer Informationen*: Jede Organisation muss in der Lage sein, Geheimnisse vor unbefugtem Zugriff zu schützen, insbesondere muss Firmenspionage und Betrug so weit wie möglich erschwert werden
- *Serviceverfügbarkeit*: Ausfälle führen zu Umsatzverlusten (Opportunitätskosten) und ggf. auch zu Schadenersatzforderungen
- *Garantie (vertraglich) zugesicherter Leistungen*: Das Einhalten von Service Level Agreements ist Grundvoraussetzung für ein Bestehen auf dem Markt
- *Einhalten gesetzlicher Vorgaben*: Bei Verstoß drohen finanzielle und persönliche Strafen, möglicherweise auch Marktausschluss
- *Schutz vor schadhafter Außendarstellung, Marktmisstrauen*: Das Vertrauen anderer Marktteilnehmer kann nachhaltig beschädigt werden

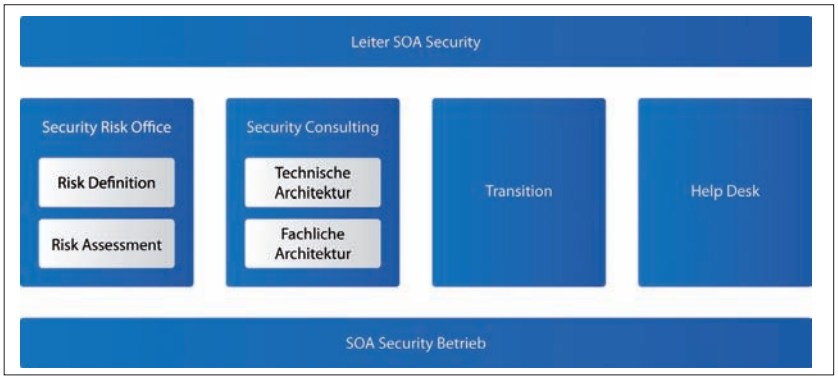

Abb. 1: Competence Center für SOA Security

ORGANISATORISCHE ROLLEN UND DOMÄNEN

Security und damit auch SOA Security ist keine isolierte, einmalige Angelegenheit, die durch die Durchführung eines einzigen Audits und das Umsetzen daraus abgeleiteter Maßnahmen durchgesetzt werden kann. Zudem verändern sich die Rahmenbedingungen ständig – neue Sicherheitslücken treten auf, Risiken werden neu bewertet, äußere und innere Veränderungsprozesse schreiten fort. Um ein konsistentes Vorgehen zu bewahren, muss eine organisatorische Grundstruktur aufgebaut werden. Kurz gesagt: Stellen Sie sich darauf ein, dass Sie das Thema Security dauerhaft begleiten wird.

Bewährt hat sich der Aufbau eines Competence Centers, um SOA Security unternehmensweit durchzusetzen. Der genaue Aufbau und die Größe dieses Competence Centers hängen natürlich von der Organisation ab, für die es arbeiten soll. Ist der Scope Ihrer SOA ein kleiner Geschäftsbereich, so werden Sie die Aufgaben des Competence Centers auf zwei bis drei Personen verteilen. In diesem Fall sollte die Bezeichnung „Competence Center" vermieden werden (anderenfalls riskieren Sie, nicht ganz ernst genommen zu werden). Unabhängig davon werden auch in einer kleinen Organisation eine Vielzahl an Aufgaben anfallen, die wir im Folgenden beschreiben. Sofern es in Ihrer Macht steht, sollte ein Competence Center für SOA Security daher unternehmensweit aufgestellt werden, damit die Aufgaben auf ein größeres Team mit spezialisiertem Know-how aufgeteilt werden können.

In der Praxis werden Sie die hier vorgeschlagene organisatorische Aufteilung an die Gegebenheiten in Ihrem Unternehmen anpassen müssen. Sollte beispielsweise bereits ein Security Competence Center bestehen, werden Sie die hier beschriebenen Aufgaben für SOA Security vermutlich in die bestehende Organisation einordnen können. Eventuell können einige Aufgaben auch von einem existierenden User Help Desk oder einem Architektur-Board übernommen werden. Wichtig ist es, die skizzierten Kernkompetenzen klar zu vergeben.

LEITER DER SOA SECURITY

Der Leiter des Security Competence Centers verantwortet ganzheitlich das Thema SOA Security in seinem Unternehmen. Als Führungskraft verantwortet er alle organisatorischen, fachlichen und technischen Aufgaben rund um das Thema SOA Security. Er leitet seine Mitarbeiter an und stellt ausreichendes Funding für die Arbeit sicher. Insbesondere ist es seine Aufgabe, das Umfeld zu managen. Dazu gehört zum einen die direkte Betreuung von Großprojekten, aber genauso auch das Reporting ins Management, um Transparenz zu schaffen. Die tägliche Arbeit wird auch dadurch geprägt sein, die mit SOA Security kommende Governance in der Praxis durchzusetzen. Hier ist insbesondere in der Anfangsphase viel Geduld und Verhandlungsgeschick von Nöten. Für Projekte stellen Security-Anforderungen häufig eine zusätzliche Last dar. Hier gilt es, die Interessen des Gesamtunternehmens mit den Möglichkeiten der einzelnen Projekte auszutarieren. Die im Folgenden beschrieben Organisationseinheiten schaffen eine sinnvolle Struktur für die Einführung, die Weiterentwick-

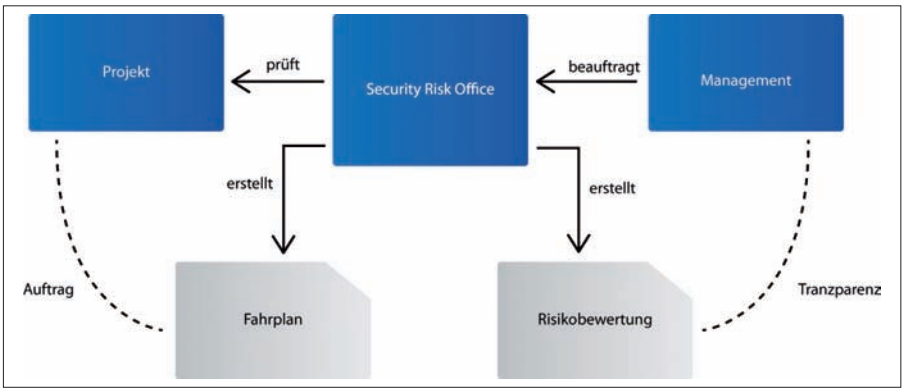

Abb. 2: Security Risk Office

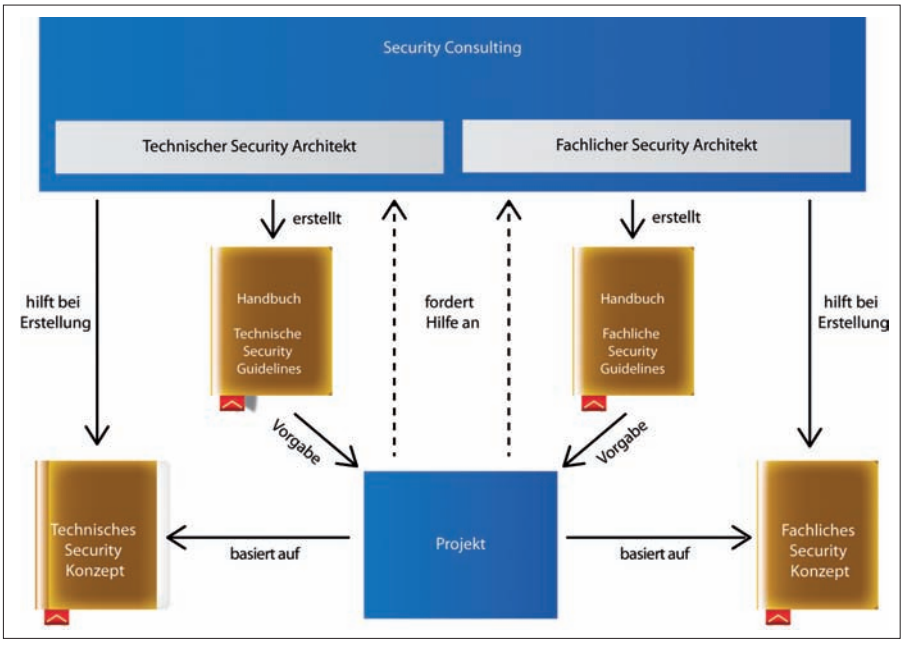

Abb. 3: Security Consulting

lung und den Betrieb einer SOA-Security-Plattform. Die verschiedenen Bereiche haben unterschiedliche fein abgestimmte Aufgabenbereiche mit Abhängigkeiten innerhalb des SOA Security Competence Center.

SECURITY RISK OFFICE

Das Security Risk Office bewertet die Risiken existierender und geplanter Projekte eines Unternehmens in Hinblick auf SOA Security. Einerseits verschafft die hierdurch erreichte Transparenz dem Thema Security mehr Aufmerksamkeit im Unternehmen. Andererseits versetzt es Projekte in die Lage, sich gezielt und planvoll in Richtung der unternehmensweit vorgegebenen Securitystandards hin zu entwickeln. Das Risk Office hat das Recht, Projekten aus der Risikobewertung resultierende Änderungsanforderungen zu stellen und deren Umsetzung zu kontrollieren. Die Zusammenarbeit zwischen Projekten und Competence Center muss im Mandat (s. u.) des Competence Centers genau festgelegt sein. Beispielsweise sind Projektgenehmigung und -abnahme typische Zeitpunkte, zu denen Governance-Aufgaben wahrgenommen werden.

SECURITY CONSULTING

Das Security Consulting unterstützt unternehmensweit Projekte bei der Einführung und Weiterentwicklung von Security. Um diese effizient zu bewerkstelligen, werden zentrale Richtlinien vorgegeben, die typischerweise in einem Intranet veröffentlicht werden. Je mehr diese Richtlinien den Charakter von Anleitungen haben, desto leichter ist es, diesen in der Praxis zu folgen und durchzusetzen. Zusätzlich kann Projekten ein Architekt zur Seite gestellt werden, der bei der operativen Umsetzung der Richtlinien mitwirkt.

TECHNISCHER SECURITY-ARCHITEKT

Der technische Securityarchitekt stellt die technischen Richtlinien zur Verfügung. Diese enthalten u. a. eine Checkliste unterschiedlicher Vorgaben, z. B. technische Standards und Konventionen, denen Projekte folgen müssen, wenn sie SOA Security umsetzen wollen. Dieses beinhaltet typischerweise auch Angaben über die im Rahmen einer Autorisierung zulässigen Token-Typen, die für die Kommunikation zwischen Service-Consumer und Token-Service bzw. Service-Provider zu verwendenden Protokolle oder auch die zur Formulierung von Autorisierungs- und Authentifizierungsregeln zu verwendende (formale) Sprache. Zusätzlich umfasst der Security Guide Vorgaben und Best Practices bezüglich der zu implementierenden sicherheitsrelevanten Aspekte der Architektur einer Anwendung bzw. eines Service sowie sonstige projekt- und sicherheitsrelevante Empfehlungen. Das umfasst insbesondere die korrekte Verwendung der SOA-Security-Plattform.

Der Prozess zur Prüfung der Vorgaben ist im Mandat des Competence Centers beschrieben – ebenso alle relevanten Kontaktpersonen des SOA Competence Center,

vorwiegend aus den Bereichen Consulting, Transition und Help Desk. Ist im Unternehmen die Rolle eines Enterprise-Architekten besetzt, stimmt sich der technische Securityarchitekt eng mit diesem ab, damit der Security Guide als Vorgabe für neue Projekte etabliert werden kann.

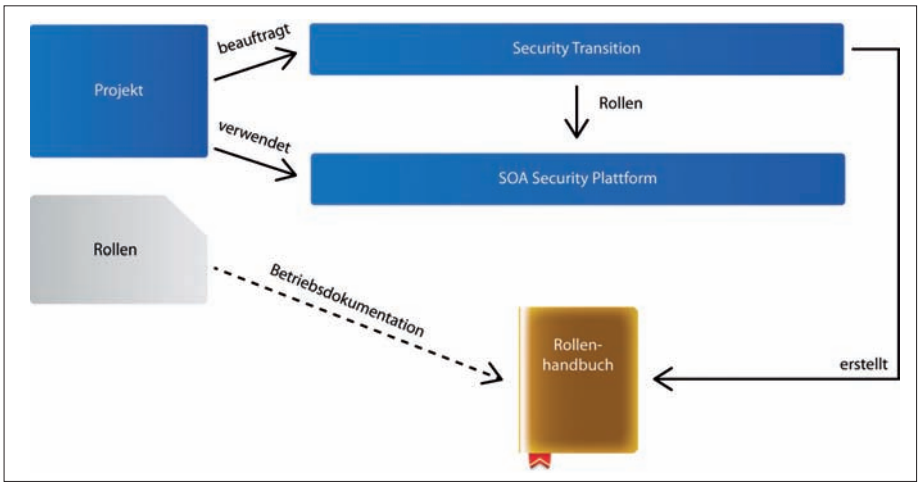

Abb. 4: Security Transition

FACHLICHER SECURITY-ARCHITEKT

Der fachliche Securityarchitekt definiert auf Grundlage der Projektanforderungen die zum Zugriff auf SOA Services nötigen fachlichen Policies. Auf Basis der zu unterstützenden Geschäftsprozesse wird ein Rollenkonzept erstellt, das die typischen Anwender (Benutzer und/oder Systeme) kategorisiert und für die Daten und Funktionen der Anwendung den nötigen Zugriffsschutz festlegt. Wir empfehlen, die betroffenen Fachbereiche möglichst früh in die Definition des Rollenkonzepts einzubinden, um Missverständnisse von vornherein zu vermeiden und ein Verständnis für das entstehende Regelwerk zu erzeugen. Das Ergebnis seiner Tätigkeit steht den Projekten zum einen zur Implementierung in der eigenen Anwendung zur Verfügung (Anpassung von Schnittstellen, Einbindung der SOA-Security-Plattform). Zum anderen dient es als Input für das Team SOA Security Transition, um die Rollen auf der SOA-Security-Plattform zu implementieren.

SECURITY TRANSITION

Security Transition unterstützt Projekte darin, auf der SOA-Security-Plattform definierte Policies zu verwalten und Rollen zu implementieren. Diese Leistung kann je nach Projektbedarf einmalig oder dauerhaft in Anspruch genommen werden. Ausschließlich dieses Team ist berechtigt, in der SOA-Security-Plattform neue Rollen zu implementieren und dem Security Help Desk zur Vergabe zu übergeben. Ziel dieser Einschränkung ist es, applikationsübergreifend Redundanzen bei Rollen und Policies zu vermeiden sowie konsistente Trainingsunterlagen, u. a. für das Security Help Desk, bereitzuhalten. Als Schnittstelle zwischen Projekten und Security Help Desk definiert die Einheit Security-Transition-Prozesse zur Verwaltung der verschiedenen Rollen. So muss beispielsweise festgelegt werden, wer in einem On-boarding-Prozess für Anwendungen bzw. Services die Autorisierung von Anwendern genehmigt.

SECURITYBETRIEB

Der Securitybetrieb unterhält die unternehmensweite SOA-Security-Plattform, die aus zentralen Bestandteilen wie Gateways, STS oder Entitlement Engines besteht oder auch dezentrale Komponenten enthält wie Security Agents, die einzelne Applikationen oder Services absichern. Die erste Aufgabe des Betriebs ist, dafür zu sorgen, dass alle Komponenten der SOA-Security-Plattform für die Nutzung bereitstehen. Dazu ist ein kontinuierliches Monitoring der Plattform erforderlich, das den Betrieb in die Lage versetzt, im Fehlerfall kurzfristig einzugreifen. Da eine SOA-Security-Plattform potenziell von allen Anwendungen in der Anwendungslandschaft gemeinsam genutzt wird, bestehen Berührungspunkte mit den Betriebsteams aller Anwendungen. Typische Aufgaben des Securitybetriebs sind Folgende:

- Zertifikate erneuern und verteilen
- Neue Regeln einspielen (siehe auch Security Transition)
- 24-x-7-Plattformbetrieb und Monitoring
- Third Level Support: Bearbeitung von Störfällen
- Erstellen eines Leitfadens zum Umgang mit Betriebsstörungen und Systemausfällen: Es ist sicherzustellen, dass alle angebundenen Anwendungen uneingeschränkt genutzt werden können

Die wichtigste Änderung im Betrieb bei der Einführung einer SOA-Security-Plattform ist die Benennung eines Plattformmanagers, der auf entsprechende Mitarbeiter zugreifen kann. Der Plattformmanager verantwortet die oben genannten Aufgaben gegenüber den Projekten.

Auf einen Aspekt sei hier noch besonders hingewiesen: In der Regel wird die SOA-Security-Plattform hochverfügbar ausgelegt sein, da ein Ausfall die Verfügbarkeit

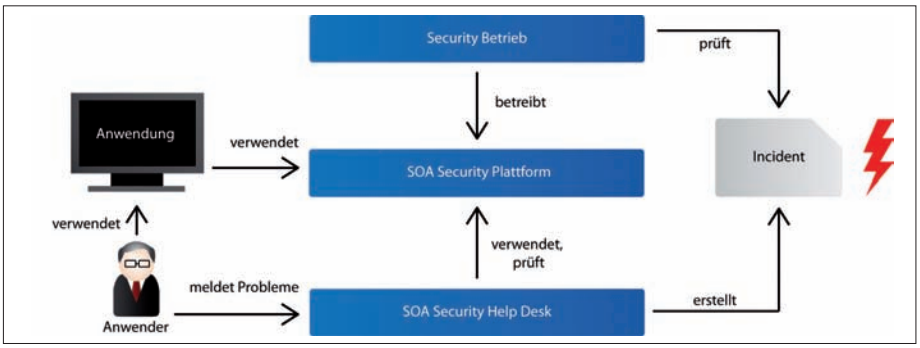

Abb. 5: Securitybetrieb

aller angebundenen Services beeinflusst. Es ist zu empfehlen, das Szenario eines Ausfalls der SOA-Security-Plattform – vollständig oder auch nur in Teilen – vorab für jede Anwendung bzw. jeden Service durchzuspielen. So kann es nach einer entsprechenden Risikobewertung durchaus sinnvoll sein, einige Services trotz fehlender Autorisierungsmöglichkeit (eingeschränkt) zur Verfügung zu stellen, um mögliche Verluste zu reduzieren. Gegebenenfalls wird vor einem solchen Hintergrund auch entschieden, Autorisierungen nur einmal am Tag abzufragen und zwischenzuspeichern, um den angemeldeten Benutzern für den laufenden Tag weiteren Zugriff zu gewährleisten. Diese Entscheidungen sind aber individuell für jede Anwendung unter Berücksichtigung der jeweils zu erzielenden Sicherheitsstufe zu treffen.

SECURITY HELP DESK

Das Security Help Desk bildet den so genannten User Lifecycle (auch User Provisioning genannt) ab. Dieser Prozess hat zum Ziel, neue oder bestehende Nutzer eines Unternehmens mit den zur Ausübung ihrer jeweiligen Tätigkeit nötigen Voraussetzungen zu versehen. Das umfasst insbesondere die Eintragung der Nutzer in einem zentralen Nutzerverzeichnis, das durch den bzw. die Identity Provider eines Unternehmens als Informationsbasis zur Erstellung von Security-Token verwendet wird, sowie die Vergabe von Rollen, die die durch die Nutzer ausgeübten Tätigkeiten widerspiegeln. In den meisten Unternehmen sind Help Desks bereits etabliert. Ebenso sind insbesondere in allen börsennotierten Unternehmen, die einer SOX-Prüfung unterliegen, Themen wie Rechtemanagement und zugehörige Beantragungsworkflows bereits bestens organisiert. Diese Organisationen sind natürlich einzubinden. Statt einen eigenständigen Help Desk aufzubauen, sollten zusätzliche Aufgaben auf vorhandene Einheiten aufgeteilt werden. Zu den neuen Tätigkeiten gehören:

- **Onboarding**, das die notwendigen Schritte umfasst, um einem neuen Benutzer (neuer Mitarbeiter, neuer Auftragnehmer, neuer Kunde oder Partner) Zugriff auf Anwendungen zu ermöglichen. In traditionellen Anwendungslandschaften müssen dazu für jede vorhandene Silo-Anwendung spezifische Rollen vergeben und Rechte eingestellt werden, oft durch Konfiguration diverser Berechtigungsdatenbanken durch anwendungsspezifische Administrationsteams. Im Gegensatz dazu wird die Authentifizierung und Autorisierung im Rahmen von Enterprise SOA Security zentral durch anwendungsübergreifende Regeln auf der Grundlage eines unternehmensweiten Rollenmodells gesteuert. Diese Vorgehensweise vereinfacht die zentrale Verwaltung durch einen anwendungsübergreifenden Help Desk bedeutend.
- **Management** der Benutzer (Name, Passwort, Verantwortlichkeiten) und deren Rollen und Rechte aufgrund veränderter Rahmenbedingungen (neue Zuständigkeiten, Abteilungswechsel usw.). Das beinhaltet die Vergabe neuer Rollen bzw. die Änderung bestehender Rollen, sodass die daraus resultierenden Berechtigungen die geänderten Bedingungen reflektieren.
- **Support** der Benutzer bei Problemen mit Systemen und Anwendungen mit typischerweise zwei verschiedenen Verantwortlichkeiten:
  - *First Level Support*: Prüfen und Lösen meist einfacher Missverständnisse und Fehlbedienungen, Zurücksetzen von Passwörtern und Ähnliches
  - *Second Level Support*: Weitergehende Untersuchung gemeldeter Incidents, die nicht direkt gelöst werden können
- **Deaktivierung** von Benutzern bei Vertragsende. Das umfasst insbesondere das Entziehen von Rollen, das automatisch auch zum Verlust der entsprechenden anwendungsübergreifenden Berechtigungen eines Benutzers führt.

Eine weitere Aufgabe ist, Auffälligkeiten aus den Supporttätigkeiten an das Security Risk Office zur weiteren Bewertung zu übergeben.

MANDAT DES COMPETENCE CENTER

Das SOA Security Competence Center benötigt ein Mandat. Das ergibt sich zum Teil aus dem Berichtsweg. Idealerweise wird der Leiter des Competence Centers an denjenigen Vorstand Ihres Unternehmens berichten, der für IT-Sicherheit zuständig ist. In den meisten Unterneh-

men reicht das aber nicht aus. Um die Arbeit des SOA Security Competence Center zum verpflichtenden Teil jedes IT-Projekts zu machen, müssen Sie dessen Arbeitsweise dokumentieren und im Governance-Handbuch Ihres Unternehmens verankern. Diese Verankerung könnte so aussehen, dass ein Security-Review zum Bestandteil jeder Projektgenehmigung wird – dass also nur Projekte, die mit dem SOA Security Competence Center zusammenarbeiten, Budget erhalten. Ebenso könnte das Governance-Handbuch vorsehen, dass nur vom SOA Security Competence Center geprüfte Projektergebnisse an den Betrieb übergeben werden können. Mit diesen beiden Governance-Checkpunkten erreichen Sie bereits eine sehr starke Einbindung. Diese offiziell einzuführen, ist allerdings nicht immer einfach. Die Governance-Checkpunkte zementieren Rechte einer zentralen Organisation gegenüber den Projekten. Diese Art von Festlegung ist in Unternehmen mit starken Fachbereichen oder ausgeprägter dezentraler Kultur häufig nur schwer durchzusetzen. Aber es ist gerade diese Änderung in der Unternehmenskultur, die den entscheidenden Unterschied zwischen einem Papiertiger und einer schlagkräftigen Organisation für SOA Security ausmacht, die Positives über Projektgrenzen hinaus bewirken kann. Hinzu kommt, dass Sie eine solche Organisation langfristig finanzieren müssen. Auch hierüber sollten Sie Festlegungen treffen. Wenn das Budget jedes Jahr aufs Neue auf dem Prüfstand steht, wird keine langfristige Arbeit möglich sein. Aus diesem Grund sollten Sie auch hierüber einen Vorstandsbeschluss erwirkt und im Mandat dokumentiert werden.

Last but not least hat ein SOA Security Competence Center den Auftrag, das Bewusstsein für Sicherheit im Unternehmen zu verbessern. Um das in der Praxis umsetzen zu können, sollte auch ein Auftrag (mit der entsprechenden Finanzierung) vorliegen, um im Unternehmen Informationen über Security zu verbreiten und Ausbildung zu betreiben. Ideal ist es, ein Intranet aufzubauen, das einen Downloadbereich für Handbücher und Securitytools umfasst, sowie eine FAQ-Liste und Schulungsunterlagen. Schulungen für technische Architekten und Businessanalysten sollten regelmäßig und aktiv angeboten werden, damit die Verbreitung des entsprechenden Know-hows im Unternehmen vorangetrieben wird.

Die Autoren dieses Artikels arbeiten seit Jahren als Berater und Trainer in diesem Bereich. Nach unserer Erfahrung benötigen Sie mindestens zwei bis drei Jahre, um Gene für SOA Security nachhaltig in Ihr Unternehmen einzuschleusen.

ZUSAMMENFASSUNG

In diesem letzten Teil unserer Artikelserie haben wir die organisatorischen Maßnahmen beschrieben, um SOA Security in der Praxis zu leben. Ausgehend von der strategischen Bedeutung von SOA Security, haben wir exemplarisch vorgestellt, wie Sie ein Competence Center für SOA Security aufbauen können. Es wurden Rollen und Tätigkeiten beschrieben, die vom Competence Center übernommen werden. Es wurden konkrete Organisationseinheiten eingeführt, die die verschiedenen Hauptaufgaben des SOA Security Competence Center verantworten. Dabei steht klar im Vordergrund, wie der Übergang von Projektanforderung zu fachlicher Analyse bis hin zu technischer Umsetzung und betrieblicher Anbindung von Anwendungen an eine SOA-Security-Plattform sichergestellt werden kann. Die vorgeschlagene Struktur des Competence Center ist als organisatorische Blaupause zu verstehen, die natürlich an die existierenden Strukturen Ihres Unternehmens angepasst werden muss. Hier spielen Randbedingungen wie Größe, existierende Gremien oder Unternehmenskultur eine wichtige Rolle. Voraussetzung für die Einführung von SOA Security ist ein umfassendes Mandat für das Competence Center, das im Auftrag der Unternehmensleitung durchgesetzt werden kann.

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 der Deutschen 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 heraus.

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.