Security Appliances in einer SOA

Sichere SOA-Infrastrukturen zu realisieren, ist und bleibt eine Herausforderung. Eine Variante, sich dieser zu stellen, ist via Security Appliances, die aus Architektursicht die sicherheitsrelevanten Aspekte einer SOA auf der Ebene der Infrastruktur lösen. Daniel Liebhart

Daniel Liebhart
ist Dozent für Informatik an der Hochschule für Technik in Zürich und Solution Manager der Trivadis AG. Er ist Mitglied des BPM/SOA-Expertenrates und Autor des Buches «SOA goes real» (Hanser Verlag) und Coautor verschiedener Fachbücher.

Eine Lösung, die basierend auf einer SOA realisiert wird, ist in fast allen Fällen ein verteiltes System. Auch wenn heute SOA meist innerhalb eines Unternehmens realisiert wird, so werden in naher Zukunft zunehmend Services eingebunden, die über Unternehmensgrenzen hinweg verfügbar sein müssen. Alle Sicherheitsaspekte, die für eine verteilte Anwendung gelten, gelten auch für eine Anwendung, die auf SOA basiert. Es existieren drei Wege zur Umsetzung dieser Sicherheitsaspekte in einer SOA: Security Standards, Security Services oder Secure SOA Infrastructure. Security Standards realisieren die Sicherheitsaspekte auf Ebene der Serviceimplementationen, respektive auf Ebene des Datenaustausches zwischen den verschiedenen Diensten. Security Services bedeuten die zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Services, die von allen anderen Komponenten einer SOA genutzt werden können. Secure SOA Infrastructure realisiert die sicherheitsrelevanten Aspekte einer SOA als Teil der Basisinfrastruktur.

Es existiert eine Vielzahl von Standards, um Sicherheitsaspekte in einer SOA abzudecken. Allen diesen Standards ist gemeinsam, dass sie auf Ebene der Serviceimplementation und des Datenaustausches realisiert werden müssen. Diese Standards basieren auf dem ursprünglichen Vorschlag aus dem Jahr 2002 von Microsoft und IBM, der auf SOAP und Webservices Security basiert. Darauf aufbauend werden Secure Conversation, Federation, Autorisation, Policy, Trust und Privacy realisiert. Diese Spezifikationen sind aktuell durch weitere Standards wie beispielsweise XACML (Extensible Access Control Markup Language), XrML (Extensible Rights Markup Language), XKMS (XML Key Management) oder SAML (Security Assertion Markup Language) für den Bereich IAA und XML-Encryption und die Integrität oder jedoch durch XML-Digital Signatures für den Bereich Vertraulichkeit erweitert

worden. Alle Sicherheitsaspekte – wie beispielsweise Identifikation, Authentisierung, Autorisierung, Integrität und Vertraulichkeit – können mit den vorhandenen Standards abgedeckt werden. Die Umsetzung dieser Standards in einer konkreten, auf SOA basierenden Lösung ist aufwendig und komplex. Sie wird durch die Tatsache erschwert, dass viele Unternehmen bestehende Anwendungen in einer SOA weiterverwenden möchten. Diese Anwendungen haben in vielen Fällen bereits Sicherheitsaspekte auf Anwendungsebene realisiert und möchten diese auch nicht verändern. Der Einsatz von Standardsoftware, wie beispielsweise eines ESB oder einer BPEL Engine oder auch eines modernen ERPs, dessen einzelne Komponenten als Webservice zur Verfügung stehen, schränkt die Möglichkeiten, komplexe Security-Mechanismen einzusetzen, stark ein. Es sind also pragmatische Ansätze gefragt, um Sicherheitsaspekte in einer SOA realisieren zu können. Idealerweise sollten sie keinen Einfluss auf den Aufbau der Lösung haben und schon gar nicht Änderungen auf Anwendungsebene nach sich ziehen.

Problematik der zentralen Security Services

Security Services bedeutet die zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Services, die von allen anderen Komponenten einer SOA genutzt werden können. Ein typisches Beispiel eines Security Services ist Identity Access Management (IAM). IAM behandelt den kontrollierten Zugriff auf Ressourcen. Dazu gehört die eindeutige Authentisierung eines zugreifenden Services als Voraussetzung für die Steuerung einer Zugriffskontrolle. Wird nun IAM als spezialisierter Dienst zentral zur Verfügung gestellt, so wird jeder Serviceaufruf darüber abgewickelt. Die einzelnen an einer auf SOA basierenden Lösung beteiligten Dienste sind davon nicht betroffen. Es sind also keine Sicherheitsmechanismen auf Ebene der einzelnen Services zu implementieren. Der Aufruf eines Dienstes erfolgt immer über den zentralen IAM-Service, der sämtliche Zugriffe kontrolliert und die angeforderten Dienste zur Verfügung stellt, respektive einschränkt. Zentrale Security Services realisieren eine deklarative oder auch Policy-basierte Sicherheit. Die Umsetzung bedeutet, dass jeder einzelne Workflow über den zentralen Security Service abgewickelt wird, also jeder Serviceaufruf bedeutet einen Aufruf des Security Services. Es existiert keine Absicherung auf Meldungsebene. Die Umsetzung bedeutet einen grossen Betreuungsaufwand für die Pflege der Rollen und der Identity-Management-Prozesse. Eine solche Realisierung ist nur für eine SOA auf Unternehmensebene zu empfehlen.

Security Appliances als Alternative

Der Einsatz von Security Appliances hat eine Vielzahl von Vorteilen gegenüber den anderen beiden Alternativen – Security Standards und zentrale Security Services. Der weitaus wichtigste Vorteil ist die sehr einfache Integrierbarkeit in eine bestehende Systemlandschaft. Ähnlich wie dedizierte Firewalls lassen sich Security Appliances gezielt an den wichtigen und sicherheitsrelevanten Stellen einsetzen und bedingen keine Änderung an der betroffenen Anwendung. Aus Sicht der Gesamtarchitektur wird Security als Teil der Infrastruktur realisiert. Dies bedeutet, dass sämtliche Sicherheitsmechanismen auf Meldungsebene realisiert werden. Daten, die zwischen den beteiligten Diensten ausgetauscht werden, werden abgesichert. Der Meldungsaustausch wird beispielsweise verschlüsselt oder die Meldungen werden mit sicherheitsrelevanten Informationen angereichert, bevor sie an das Zielsystem weitergeleitet werden. Eine vielversprechende Realisierung ist der Einsatz von SOAP Firewalls. Sie können XML-Schema-Validierung, digitale Zertifikate und Verschlüsselung/Entschlüsselung in Echtzeit durchführen.

Die Konsequenzen aus Architektursicht

Interessant ist der Einsatz von Security Appliances aus Sicht der Gesamtarchitektur. Nicht nur, dass die Anwendungen, Prozesse und anderen typischen Komponenten einer SOA von den sicherheitsrelevanten Mechanismen entlastet werden, sondern auch, dass die Sicherheit klar auf einer einzigen Ebene der Gesamtarchitektur realisiert wird, nämlich auf der Infrastrukturebene. Dies setzt allerdings voraus, dass die einzelnen Bestandteile einer auf SOA basierenden Anwendung über standardisierte Webservice-Schnittstellen miteinander verbunden sind. Nur so können einerseits die vielen Tools – beispielsweise für die automatisierte Prozess- und Regelsteuerung, die Registrierung und Verwaltung von Diensten oder andere Standardsoftware – und Produkte mit bestehenden Komponenten kombiniert werden. Und nur so kommen Security Appliances zur vollen Wirkung.

Inzwischen existieren eine Reihe von Appliances für SOA Security auch schlicht SOA Appliances genannt. Hersteller wie IBM, Layer 7 Technologies, Cisco und andere bieten diese Produkte in einem breiten Preissegment an. Sie entsprechen dedizierten Hardware Firewalls, die seit Jahren erfolgreich in Unternehmen eingesetzt werden. Sie unterstützen eine Vielzahl von WS-Security Standards sowie die anderen gängigen Protokolle wie beispielsweise Kerberos, SAML, PKI CA und viele andere mehr. Darüber hinaus haben sie einen sehr interessanten Nebeneffekt, die Verschlüsselung und Komprimierung auf Hardwarebene beschleunigt den Datenaustausch erheblich. Dies kann sogar so weit gehen, dass SOA Appliances als Hardware ESB eingesetzt werden. Allerdings sind die meisten Appliances nicht gerade billig. Werden jedoch die reduzierten Betriebskosten durch standardisiertes und zentrales Management sowie die reduzierten Entwicklungs- und Anpassungskosten mit eingerechnet, so lohnt sich der Einsatz dieser Geräte in sehr vielen Fällen.

Pragmatische Ansätze sind gefragt

Viele Unternehmen setzen zunehmend auf SOA als Standardarchitektur. So können Lösungen standardisiert, Kosten sparend und flexibel umgesetzt werden. Die Tatsache, dass bestehende Anwendungen und Standardprodukte zu einem funktionierenden Ganzen kombiniert werden, erschwert die Umsetzung von Sicherheitsaspekten auf Ebene der einzelnen Dienste. Es sind pragmatische Ansätze gefragt, um Sicherheitsaspekte in einer SOA realisieren zu können. Der Einsatz von Appliances im Rahmen einer SOA ist eine vielversprechende Lösung, ohne dass Anwendungen und SOA-Komponenten mit Security-Aspekten überladen werden. ■