www.bt-magazin.de 2.2011 Heft 5 Deutschland: € 14,90 Österreich: € 16,80 Schweiz: sFr 29,80 Luxemburg: € 16,90

Business Technology

Business Technology

Architektur & Management Magazin

Peter Schaar: „Datenschutz setzt die Spielregeln."

Expertenwissen für IT-Architekten, Projektleiter und Berater

SICHERHEIT

IT-Sicherheit integral betrachtet

Data Loss Protection

Enterprise Wide Integration Security

Alles sicher oder was?
Die BSI-Sicherheitsanforderungen an Cloud-Anbieter

Rechte und Rollen
Zentrales Rollen- und Rechtecockpit für SOA-Applikationen

Business Continuity Management
Sicherung kritischer Wertschöpfungsprozesse

Schatzkammer Datenbank
Sicherheitsstrategien für Datenbanken

4 191858 414906 02

Organisatorische Maßnahmen

Einführung in XML-Gateways

Die Artikelserie „Enterprise SOA Security“ in den letzten vier Ausgaben dieses Magazins hat bereits die Grundlagen von Web Services Security erläutert. Im vorliegenden Artikel gehen wir nun auf eine Implementierungsstrategie für Security ein, die insbesondere für abteilungs- und unternehmensübergreifende Web-Services-Kommunikation vorteilhaft ist.

AUTOREN: MAMOON YUNUS UND DIRK KRAFZIG

Zu den Zielen einer serviceorientierten Architektur (SOA) gehören lose Kopplung und Flexibilität. SOA ermöglicht es Applikationen, auf einfachste Weise auf Services zuzugreifen, die Daten und Geschäftsfunktionen zentral bereitstellen. Flexibilität und Einfachheit einer SOA stehen aber häufig im Widerspruch zur Sicherheit. Während die gewünschte Einfachheit zu einer möglichst offenen SOA führt, wirken Sicherheitsanforderungen in die entgegengesetzte Richtung. Um den Erfolg einer SOA dennoch sicherzustellen, müssen die unterschiedlichen Anforderungen sorgsam ausbalanciert werden. Ein XML-Gateway ist eine IT-Infrastrukturkomponente, die dabei hilft, den einfachen Zugriff auf Services zu erlauben, ohne dabei die Sicherheit zu vernachlässigen. Dieser Artikel liefert Best Practices für den Einsatz von XML-Gateways und zeigt, wie z. B. Datenintegrität und -vertraulichkeit gewährleistet werden können, ohne die Komplexität für die Anwendungsentwickler und den Betrieb zu erhöhen.

Ein XML-Gateway wird typischerweise als Hardware Appliance implementiert. Es kontrolliert den Zugriff auf Services und schützt Informationen durch Verschlüsselung auf Datenebene, stellt Integrität durch Signaturen sicher und kontrolliert den Fluss von Unternehmensinformationen. Dieser Artikel betrachtet XML-Gateways aus drei Perspektiven (**Abbildung 1**):

- Servicevirtualisierung
- Vertraulichkeit und Integrität von Daten
- Kontrolle der Datenflüsse und Auditing

SERVICEVIRTUALISIERUNG

Servicevirtualisierung ist eine wichtige Praktik in einer SOA. Hier geht es darum, von der konkreten Implementierung eines Service zu abstrahieren und die lose Kopplung zu erhöhen. In der Regel möchte man einzelne Operationen verschiedener Services zu neuen Services kombinieren, die unter einer neuen WSDL den Service-Consumern angeboten werden. **Abbildung 2** zeigt, wie Servicevirtualisierung über mehrere Providersysteme dadurch erreicht wird, dass ein XML-Gateway als Intermediary zwischen Providern und Consumern fungiert. Anstatt Services direkt von vielen Providern zu beziehen, können vornehmlich externe Service-Consumer auf sie zugeschnittene virtuelle Services von dem Intermediary beziehen. Dies kann aus Sicht des Consumers dann durch eine einzelne WSDL über einen einzelnen physischen Endpunkt geschehen. Servicevirtualisierung erlaubt es Unternehmen, spezifische Services, die z. B. von ihren Kunden benötigt werden, selektiv anzubieten, statt sämtliche Services des Unternehmens veröffentlichen zu müssen. **Abbildung 2** zeigt ein Beispiel, in dem interne Consumer autorisiert sind, die Services A bis E zu verwenden. Ein externer Consumer darf in dem Beispiel die Services D und F verwenden. Ein XML-Gateway agiert hier als zentraler Kontrollpunkt, der den Zugriff auf Services durch Virtualisierung steuert.

VORTEILE DER SERVICEVIRTUALISIERUNG

Konsistenz: Virtualisierung erlaubt es, Consumern eine einzelne kohärente WSDL bereitzustellen, die ausschließ-

lich Serviceoperationen enthält, die für den Consumer interessant sind, und auf die der Consumer auch zugreifen darf.

Sicherheit: Die virtuelle WSDL kann selektiv Serviceoperationen, für die kein Zugriff besteht, ausblenden. Die wirklichen WSDLs und Endpunkte bleiben verborgen und nur die Endpunkte, die vom XML-Gateway angeboten werden, sind sichtbar. Die Angriffsfläche auf das Unternehmen wird kleiner und man kann alle Kräfte darauf konzentrieren, das XML-Gateway zu schützen, um unerlaubten Zugriff zu verhindern.

Produktivität: Servicevirtualisierung verbessert die Produktivität durch das Bereitstellen von Serviceinterfaces, die auf den Consumer zugeschnitten sind.

Anforderungen an XML-Gateways für die Virtualisierung: Um großen Unternehmen als Virtualisierungsschicht für ihre Servicelandschaften zu dienen, müssen XML-Gateways zunächst einmal in hohem Maße robust und zuverlässig sein. Der unterbrechungsfreie 7x24-Betrieb im Rechenzentrum ist grundlegende Voraussetzung. Für den Umgang mit Web Services müssen XML-Gateways zudem herausragende Fähigkeiten haben. Dabei sind folgende Eigenschaften besonders wichtig:

- *Integration mit Identity-Management-Systemen*: Für die Authentifizierung von Absendern einer Nachricht – das ist die Voraussetzung für viele nachfolgende Sicherheitsmechanismen – muss ein XML-Gateway nahtlos mit den Identity-Management-Lösungen integrierbar sein, die im Unternehmen bereits existieren.
- *Identity Bridging*: Ein XML-Gateway muss ausgeklügelte Mechanismen unterstützen, um Security Tokens verarbeiten zu können. Das ist insbesondere wichtig, da beim Übergang von einer Organisationseinheit zur nächsten damit gerechnet werden muss, dass verschiedene Mechanismen zum Einsatz kommen, um die Benutzeridentität und andere Security-relevante Daten zu beschreiben.
- *Management komplexer WSDLs*: Fähigkeit zum Parsen, Mergen und Verwalten vieler zusammengesetzter WSDLs und Schemas. Dabei müssen insbesondere Kollisionen und Inkompatibilitäten beim Mergen von WSDLs bearbeitet werden können.

Servicevirtualisierung mit einer feingranularen Zugriffskontrolle ist entscheidend für die Skalierbarkeit einer SOA. Die unkontrollierte Verbreitung von Services kann sonst schnell im Chaos enden. Ein XML-Gateway kann durch Servicevirtualisierung dazu beitragen, die ansteigende Komplexität innerhalb der SOA zu kontrollieren und zu managen. Die Integration von Identity-Management-Systemen geht Hand in Hand mit der Servicevirtualisierung.

Abb. 1: Ein XML-Gateway kann aus unterschiedlichen Motiven eingesetzt werden

VERTRAULICHKEIT UND INTEGRITÄT DER DATEN

Vertraulichkeit und Integrität sind die Eckpfeiler jeder unternehmensweiten SOA. Um Vertraulichkeit und Integrität von Nachrichten zu erreichen, ermöglichen SOAP und dazugehörige Web-Services-Standards die Verschlüsselung und das Signieren von Nachrichten unabhängig vom Transportprotokoll wie z. B. HTTP, JMS, FTP etc. Damit liegt die Sicherheit von Nachrichten nicht mehr in der Hand der Transportschicht und Intermediaries sondern allein im Web Services Stack.

XML-Gateways können dazu verwendet werden, die Verschlüsselung und Signatur von Daten sicherzustellen. **Abbildung 3** erläutert ein typisches XML-Gateway. Bei ausgehendem Datenverkehr wird eine Nachricht zuerst verschlüsselt und dann signiert, bevor sie an den Service-Provider geschickt wird. Bei eingehendem Datenverkehr wird zunächst die Verifikation der Signatur durchgeführt, um sicherzustellen, dass auf dem Transportweg keine Änderungen der Nachricht vorgenommen wurden. Danach wird die Nachricht entschlüsselt und an den Service-Provider geschickt.

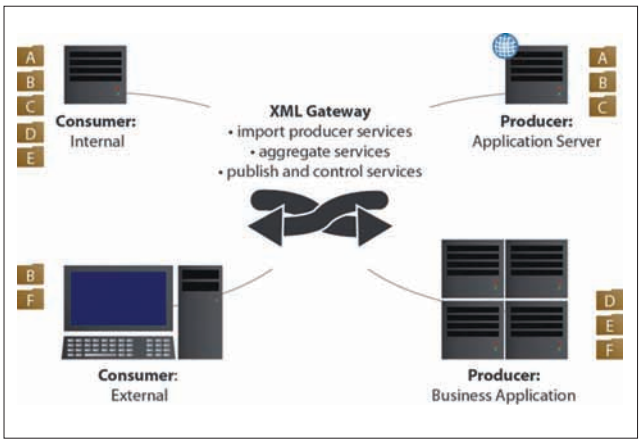

Abb. 2: Servicevirtualisierung durch XML-Gateways

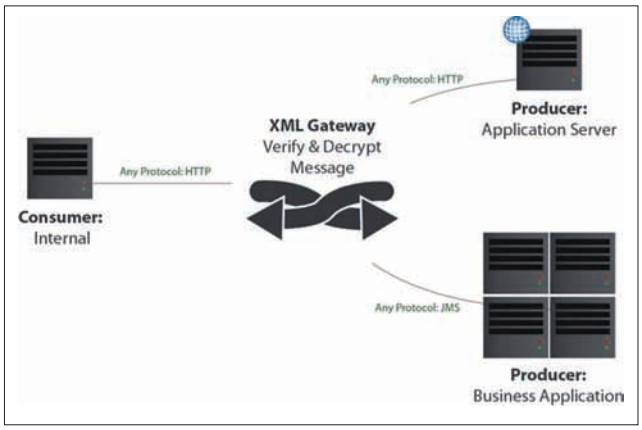

Abb. 3: Vertraulichkeit und Integrität von Daten

VORTEILE VON VERTRAULICHKEIT UND DATENINTEGRITÄT

Vertraulichkeit und Datenintegrität verschaffen viele wichtige Vorteile.

Konsistenz: Durch das Zentralisieren von Sicherheitsrichtlinien kann das XML-Gateway einen hohen Grad an Konsistenz und Kontrolle sicherstellen. Serviceimplementierungen werden dadurch unabhängig von den zu Grunde liegenden Sicherheitsrichtlinien. Das XML-Gateway sorgt transparent für die Durchsetzung aller festgelegten Sicherheitsrichtlinien.

Sicherheit: Sicherheit auf Datenebene ist unabhängig vom Transportprotokoll. Hochsensible Daten innerhalb einer Nachricht können optimal geschützt werden, während öffentliche Daten unverschlüsselt bleiben können. Die Sicherheit der Daten wird durch das XML-Gateway garantiert, auch wenn einzelne Services verwundbar sind.

Produktivität: Durch das Zentralisieren von Sicherheitsrichtlinien auf dem XML-Gateway werden Entwickler davon freigestellt, sich mit diesen befassen zu müssen und entsprechenden Code zur Umsetzung der Sicherheitsrichtlinien zu schreiben. Abgesehen davon, dass hierfür Zeit und Geld benötigt wird, ist die Implementierung von Security-Mechanismen alles andere als einfach. Wie in **Abbildung 3** gezeigt wird, können sich Entwickler auf die Entwicklung der Kernfunktionalität konzentrieren. Dadurch wird die Produktivität vom Entwicklungsteam erheblich gesteigert, ohne Kompromisse bei der Sicherheit eingehen zu müssen.

Anforderungen an XML-Gateways für Vertraulichkeit und Integrität: Um die Vertraulichkeit und Integrität der Daten sicherzustellen, muss ein XML-Gateway folgende Anforderungen erfüllen:

- *Unterstützung möglichst vieler Standards*: Eine Nachricht, die verschlüsselt wurde, muss auch wieder entschlüsselt werden. Ebenso muss eine Signatur, die von einer Applikation erstellt wurde, durch eine andere Applikation verifiziert werden können. Da man in der Regel nicht alle Service-Consumer und Service-Provider einer SOA unter eine gemeinsame Governance stellen kann, wird man auch im Security-Bereich auf Heterogenität stoßen. Das XML-Gateway dient hier als Vermittler, der die Standards auf beiden Seiten verstehen und entsprechend übersetzen können muss.
- *Robustes PKI-Management*: Verschlüsselung und Entschlüsselung sowie Signatur und Verifikation basieren auf PKI (*Public Key Infrastructure*). Ein XML-Gateway muss den Lebenszyklus der Schlüssel (generieren, verteilen und erneuern) unterstützen. Zur Verbesserung der Sicherheit verwenden XML-Gateways Hardwaremodule, um private Schlüssel vor unberechtigtem Zugriff zu schützen. Solides PKI-Management, verbunden mit Hardwaremodulen, ist eine Basisanforderung für XML-Gateways, die an kritischer Stelle in Unternehmen eingesetzt wird.
- *Performancebeschleunigung*: Kryptografische Operationen, die für die Verschlüsselung und Entschlüsselung von Nachrichten notwendig sind, verbrauchen viel Rechenzeit. Um in großem Maß skalieren zu können, sind Standardprozessoren nicht geeignet. Es werden spezialisierte kryptografische Prozessoren benötigt. Ein XML-Gateway, das solche Operationen für Service-Consumer und Service-Provider durchführt, muss über Hardwarebeschleunigung verfügen, um die erforderliche Skalierbarkeit zu ermöglichen und nicht zum Nadelöhr der Architektur zu werden.

Entwickler von Geschäftslogik mit Sicherheitsanforderungen zu belasten, ist auf lange Sicht eine falsche Strategie. Sie führt zu einem außerordentlichen Aufwand in der Wartung der Serviceimplementierung und setzt die SOA-Sicherheitsrisiken und Probleme in der Interoperabilität aus. Das Trennen von Sicherheitsrichtlinien von der Serviceimplementierung und die Zentralisierung der Richtlinien kann durch ein XML-Gateway sichergestellt werden.

KONTROLLE DER DATENFLÜSSE UND AUDITING

In einer SOA können Informationen einfach zwischen Applikationen fließen. Die Applikationen sind nicht notwendigerweise intern; einer der großen Vorteile von SOA ist die Einbindung externer Partner. Mit der Vereinfachung des Informationsflusses steigt automatisch der Bedarf an Kontrolle. Dabei ist das Filtern und Archivieren von Nachrichten eine wichtige Anforderung.

Mit Nachrichtenfilterung kann man sicher stellen, dass keine bösartigen Nachrichten in das Unternehmen

eindringen können. Ebenso können Informationslecks verhindert werden, wie das versehentliche oder absichtliche Versenden von Nachrichten mit sensiblem Inhalt, der nicht aus dem eigenen Unternehmen herausgetragen werden sollte. Zusätzlich möchte man den Datenfluss mit externen Partnern auch dokumentieren, um jederzeit Rechenschaft vor internen und externen Revisoren abgeben zu können.

Wie **Abbildung 4** zeigt, bietet ein XML-Gateway die Möglichkeit, Nachrichten zu filtern und zu archivieren. Das XML-Gateway fängt Nachrichten ab und sendet sie erst nach einer Inspektion bzw. nach der Archivierung weiter.

VORTEILE DER DATENFLUSSKONTROLLE

Konsistenz: Durch Zentralisieren des Filterns und Archivierens kann ein konsistentes Regelwerk im gesamten Bereich der SOA angewendet werden. Damit kann zentral gesteuert werden, welche Nachrichten in das Unternehmen hinein- und herausfließen, und darüber hinaus eine Prüfung der Umsetzung erlaubt werden.

Sicherheit: XML-Gateways agieren als Firewalls für Nachrichten in einer SOA. Durch ihre Fähigkeit, den Inhalt zu inspizieren, erlauben es XML-Gateways, eingehenden Datenverkehr auf bösartigen Inhalt zu untersuchen und nur saubere Nachrichten durchzulassen.

Produktivität: XML-Gateways entbinden Anwendungsentwickler von der Verpflichtung Nachrichten zu loggen und Inhalte zu filtern. Mit einfachen Maßnahmen – auch ohne zu kodieren – können Richtlinien umgesetzt werden.

ANFORDERUNG AN XML-GATEWAYS FÜR DIE DATENFLUSSKONTROLLE

- *Bidirektionale Kontrolle von Nachrichten*: Sowohl eingehende als auch ausgehende Nachrichten müssen vom XML-Gateway verarbeitet werden. Typischerweise werden eingehende Nachrichten auf bösartige Inhalte untersucht und archiviert. Ausgehende Nachrichten werden üblicherweise auch auf sensitive Informationen geprüft, bevor ihre Weiterleitung erlaubt wird.
- *Feingranulare Steuerung der Archivierung von Nachrichten*: XML-Gateways müssen die Fähigkeit haben, komplette Nachrichten oder auch einzelne Teile daraus zu speichern.
- *Flexible Konfiguration*: XML-Gateways müssen ein hohes Maß an Flexibilität zur Konfiguration der Richtlinien für das Filtern und Archivieren von Nachrichten bieten. Sie müssen es gestatten, beliebige Kriterien basierend auf dem Inhalt der Nachricht heranzuziehen.

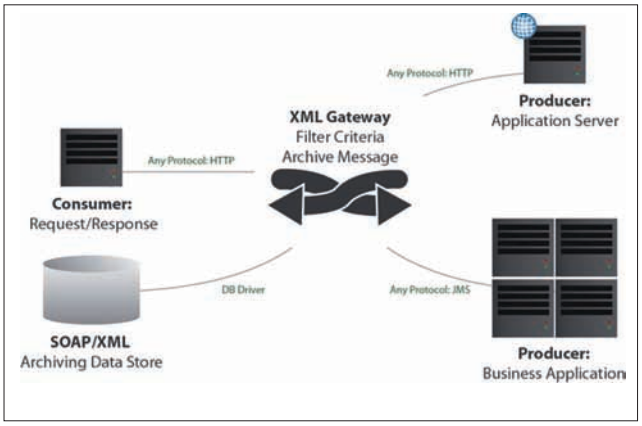

Abb. 4: Kontrolle der Datenflüsse durch XML-Gateways

Ähnlich einem E-Mail-System soll ein XML-Gateway eingehende und ausgehende Nachrichten verarbeiten. Schadhafte Inhalte müssen ausgefiltert werden. Ebenso ist eine Protokollierung des Nachrichtenverkehrs erforderlich.

ZUSAMMENFASSUNG

Ein XML-Gateway ist eine zentrale Infrastrukturkomponente einer SOA mit der Fähigkeit, Services sicher zu integrieren. Es kontrolliert den Zugang zu Services, schützt Informationen durch Verschlüsselung auf Datenebene, stellt die Integrität von Nachrichten durch Signaturen sicher und steuert den Austausch sensitiver Nachrichteninhalte. Typischerweise wird ein XML-Gateway als Hardware Appliance installiert. Durch die Hardwareunterstützung arbeitet ein XML-Gateway um ein Vielfaches schneller und sicherer als softwarebasierte Lösungen.

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" haben viel Aufmerksamkeit auf sich gezogen. Derzeit arbeitet Dr. Krafzig in einem strategischen SOA-Programm bei einem Mobilfunkanbieter an dem Thema Security.

Mamoon Yunus ist CEO von Crosscheck Networks, einem führenden Technologie-Anbieter für Cloud und Web Service Infrastrukturen. Als SOA Pionier und Gründer von Forum Systems hat er wichtige Techniken für XML Appliances patentieren lassen. Er besitzt zwei Abschlüsse vom MIT. InfoWorld hat ihn 2004 als einen von vier "Up and coming CTOs to watch" ausgezeichnet.