Generali optimiert Webservice Security mit IBM DataPower Appliances

Die IBM WebSphere DataPower Security Gateways sorgen für sehr performante und sichere XML-Verarbeitung

GENERALI Informatik Services

Überblick

Die Anforderung

Der ‚Versicherungsbetrieb der Zukunft' erfordert flexible Abläufe und die direkte Integration der Geschäftsprozesse von Partnern mit der Anwendungslandschaft der Generali Deutschland Gruppe. Um den Geschäftspartnern mehr Leistung über vielfältige Kanäle der hauseigenen Internetplattform anbieten zu können, muss die Generali den Zugriff auf die Geschäftsfunktionen über Webservices auf besondere Weise absichern.

Die Lösung

Generali integrierte IBM DataPower Appliances in ihre SOA-Umgebung: performant, zuverlässig, leicht in die vorhandene Architektur einpassbar und konform mit Webservice- und Security-Standards.

Die Generali ist die zweitgrößte Erstversicherungsgruppe in Deutschland. Unter ihrem Dach arbeiten namhafte Versicherer und Finanzdienstleistungsunternehmen. Durch das Internet ändern sich die Geschäftsprozesse bei den Versicherungsunternehmen grundlegend. Kunden und Geschäftspartner führen vielfältige Aktionen selbstständig durch; die Mitarbeiter in den Kundenservicecentern oder in den spezialisierten Fachbereichen greifen in unterschiedlicher Breite und Tiefe auf Anwendungen, Informationen und Daten zu; Prozesse werden automatisiert. Für viele Einzelprozesse lassen sich aber die gleichen internen und externen Services nutzen. „Für den ‚Versicherungsbetrieb der Zukunft' mit seinen komplexen Bearbeitungsprozessen, vielfältigen Ein- und Ausgangskanälen und flexiblen Abläufen haben wir eine serviceorientierte Architektur eingeführt", erklärt Dr. Stefan Bühne, IT-Architekt bei der Generali Deutschland Informatik Services GmbH in Aachen (GD-Informatik). „Geschäftsprozesse sollen möglichst dort bearbeitet werden, wo dies besonders wirtschaftlich erfolgen kann, das heißt dort, wo sie anfallen." Mit einer serviceorientierten Architektur brauchen einzelne fachliche oder technische Services nur einmalig eingerichtet werden, um sie dann den jeweiligen Anwendungen zur Verfügung zu stellen. Dadurch lassen sich teure Redundanzen und unnötige Komplexität vermeiden. Die Servicebausteine lassen sich flexibel neu kombinieren, je nachdem, ob es interne Umstrukturierungen, erweiterte gesetzliche Anforderungen oder geänderte Kundenwünsche gibt. Dr. Bühne: „Die IT-Sicherheit steht damit vor völlig neuen Herausforderungen, zum Beispiel wenn, wie bei Generali, externen Geschäftspartnern Zugriff auf interne Webservices gewährt werden soll."

Spezialisiertes Service Gateway erforderlich

Die GD-Informatik ist der IT-Dienstleister für die Generali Deutschland Gruppe und für Gesellschaften der Assicurazioni Generali S.p.A in der Region Central East. Mit rund 1.200 Mitarbeitern, zwei Standorten in Hamburg und in Aachen sowie einem Umsatz von rund 370 Millionen Euro (2009) gehört sie zu den wichtigsten IT-Dienstleistern in Deutschland. Zwei IBM System z10 Mainframes bewältigen bis zu 32 Millionen Host-Online-Transaktionen täglich. Der Plattenspeicher umfasst mehr als 1.000 Terabyte an Daten. Selbstverständlich ist die Internet- und Intranetplattform in einer Trusted Zone geschützt. Dialoganwendungen und Webservices sind technologisch unterschiedlich angebunden. Durch diese Kopplung unterschiedlichster Systeme reicht es nicht mehr aus,

Der geschäftliche Nutzen

- Die sichere Kontrolle und Verschlüsselung von XML-Nachrichtenflüssen ermöglicht die zuverlässige und autorisierte Kommunikation mit Geschäftspartnern, die einzelne Geschäftsfunktionen von Generali in ihren eigenen Prozessen nutzen möchten.
- Der hohe Durchsatz und die Stabilität bei der Verarbeitung komplexer XML-Dokumente ist Voraussetzung für die effiziente, verlässliche Zusammenarbeit mit Partnern.
- Die Verwaltung, Kontrolle und Überwachung von Sicherheitsrichtlinien (Governance) erfolgt konsistent und transparent auf einem einheitlichen Gateway.
- Durch die Umsetzung von wiederverwendbaren Sicherheitsstufen für einzelne Webservices lassen sich Änderungen und Anpassungen ohne Redundanzen betriebssicher und transparent vornehmen.
- Die saubere Zuordnung und Zentralisierung der Sicherheitsfunktionen auf eine robuste Geräteeinheit sorgt für niedrige Administrationskosten und einen problemlosen Betrieb.

nicht autorisierte Zugriffe mit gewöhnlichen SSL-Verfahren abzuwehren. Dr. Bühne: „Für die Absicherung von Dialoganwendungen setzen wir IBM Tivoli Access Manager mit WebSEAL ein, zum Beispiel für unser GINA-Portal, das wir für den Außendienst aufgebaut haben.“ Dagegen sind Inhalte, die über Webservices transportiert werden, als XML-Dokumente technisch komplexer, aufwändiger in der Verarbeitung und bieten zu viele Angriffsflächen, um sie performant über WebSEAL abzusichern und zum Beispiel Denial-of-Service-Attacken abzuwehren. „Einige unserer Geschäftspartner wollten Services aber direkt nutzen, ohne dabei über das Internet-Portal zu gehen. Für die Webservices wollten wir unbedingt ein gesondertes Verfahren nutzen, das für diesen speziellen Weg optimal ausgelegt ist.“ Dieses Service Gateway mit schneller XML-Verarbeitung wurde mit IBM Websphere DataPower XML Security Gateway XS40 eingeführt, eine spezielle SOA Appliance in Form von kompakten Geräten für den Einschub in 1,75-Zoll-Standard-Racks.

Einheitliche Authentifizierungsverfahren

IBM ist der bewährte Partner der GD-Informatik, der sowohl die Versicherungswirtschaft allgemein als auch die Anforderungen der GD-Informatik sehr gut kennt. Außerdem legt die GD-Informatik besonderen Wert auf klare Verantwortlichkeiten, wenn unterschiedliche Produkte miteinander funktionieren müssen. Dr. Bühne: „Damit lag die Präferenz für eine IBM Lösung auch für Webservice Security auf der Hand.“ Das entscheidende Argument aber war: In der gesamten Anwendungslandschaft bei der Generali wird das Single-Sign-on-Zugriffsverfahren LTPA (Lightweight Third-Party Authentication) zur Authentifizierung eingesetzt, ein Merkmal von IBM WebSphere-Produkten. „Damit passen IBM DataPower Appliances perfekt in unsere Sicherheitsarchitektur“, unterstreicht Dr. Bühne. „2008 nahmen wir an einem Proof of Technology-Workshop zu DataPower bei IBM teil, nachdem unsere Kriterien feststanden. So konnten wir in kompakter Form den praktischen Einsatz kennenlernen.“

Bis Ende 2009 wurden acht DataPower Security Gateways angeschafft. Sie sind für die produktive Infrastruktur je Rechenzentrum und je Zugang aus dem Internet bzw. dem lokalen Netzwerk redundant vorhanden, um die Hochverfügbarkeit und den Durchsatz sicherzustellen. Weitere Geräte bieten einen analogen Zugang zur Infrastruktur der Testebenen. Das Service Gateway übernimmt die technischen Prüfungen der Authentifizierung und der syntaktischen Korrektheit des Serviceaufrufs sowie die XML-Verschlüsselung und kann dabei zum Beispiel zwischen technischen

Lösungskomponenten

Software/Hardware

- IBM WebSphere DataPower XML Security Gateway XS40

IBM Business Partner

- Unterstützung bei der Implementierung und Schulungen durch BLUECARAT AG

„Es ist äußerst sinnvoll, robuste, durchsatzfähige und spezialisierte Geräte für die Sicherheit im Bereich Webservices einzusetzen. Die IBM DataPower Appliances passen einfach."

— Dr. Stefan Bühne, IT-Architekt, Generali Deutschland Informatik Services GmbH, Aachen

und personenbezogenen Benutzern unterscheiden. Die Einführung hat der Kölner IBM Business Partner BLUECARAT AG unterstützt. Das Unternehmen ist unter anderem spezialisiert auf Pilotierung, Einführung und Integration von Services über XML-basierte Schnittstellen. „Für die Details der Konfiguration und Implementierung der Appliances waren die Fachleute von BLUECARAT für uns der ideale Coaching-Partner, und wir waren mit der Zusammenarbeit sehr zufrieden." Die sorgfältige Arbeit an der Architektur zahlte sich aus: „Die Entscheidung war richtig, die IBM Appliance-Technologie ist sehr gut. Wir haben bis heute nichts an dem Konzept ändern müssen. Die Teilnahme an einem IBM Proof of Technology-Workshop können wir nur empfehlen."

Keine Redundanzen, klare Verantwortlichkeiten

Sukzessive hat die GD-Informatik inzwischen neue Webservices eingeführt und sie für externe und interne Geschäftsprozesse zur Verfügung gestellt. Alle Services bauen auf der vorhandenen Sicherheitsarchitektur auf. Die Pflegeprozesse gestalten sich schlank. „Das liegt zum einen daran, dass die Appliance eine wirklich gute Bedienoberfläche hat, und zum anderen daran, dass wir von Anfang an ein klares Einsatzkonzept verfolgt haben", sagt Dr. Bühne. Denn die Lösung sollte sich auch in der Folgezeit sehr effizient betreiben lassen. Eine Besonderheit der Appliances liegt auch darin, dass sie eine Kombination von Hardware und Software darstellen und personelle Verantwortlichkeiten nicht ohne weiteres automatisch zugeordnet werden können. „In Analogie zum Tivoli Access Manager zählen wir die DataPower Appliances zu den IBM Software-Komponenten und ganz bewusst nicht zu den Netzwerkkomponenten", erläutert Dr. Bühne. „Mit betrieblichen Anweisungen regeln wir die Verantwortlichkeiten bei uns im Haus unmissverständlich. Diese organisatorische Klarheit ist unverzichtbar für die tägliche Betriebssicherheit."

Besonders positiv wertet die GD-Informatik die ‚Objektorientierung' der IBM DataPower Appliances. Jedem einzelnen Service wird eine der unternehmensweit gültigen Sicherheitsstufen zugewiesen. Mehrere XML-Firewalls nutzen innerhalb einer Sicherheitsstufe immer dieselben Verarbeitungsregeln. Diese sind so immer konsistent und gewährleisten stets das entsprechende Sicherheitsniveau für verschiedene Webservices. „Diese Prüfregeln können wir als eigenes Objekt anlegen und brauchen sie nicht zu duplizieren", erklärt Dr. Bühne. „Wenn es Änderungen bei den Sicherheitsregeln gibt, müssen sie nur ein einziges Mal für alle sich darauf beziehenden Webservices vorgenommen werden. So erzielen wir eine absolute Stimmigkeit bei den Sicherheitsprüfungen."

Die Administration erfolgt komfortabel. In einer Appliance können in verschiedenen Domänen mehrere komplett unabhängige Konfigurationen gepflegt werden. Das nutzt die GD-Informatik beispielsweise für den Aufbau von Testumgebungen, die dann problemlos in den Produktivbetrieb übernommen werden können. Dazu können Konfigurationen von der Testebene exportiert und auf einer höheren Ebene wieder importiert werden (Staging-Verfahren). Ein weiterer Vorteil ist die einfache Fehlersuche: Einzelne Requests können mittels Probing aufgezeichnet werden. So wird sofort ersichtlich, welche Daten auf der DataPower Appliance durchgelaufen sind. Fehlersituationen können extrem schnell lokalisiert werden. Dr. Bühne: „Unsere bisherigen Praxiserfahrungen haben gezeigt, dass es nie an den DataPower-Geräten selbst gelegen hat. Die Boxen senden eine Vielzahl

von aussagekräftigen, differenzierten Meldungen, so dass gezielt nach den Ursachen gesucht werden kann; zum Beispiel, an welcher Stelle im Gesamtsystem es Versionskonflikte gibt. Insgesamt unterstützen die Geräte eine Vielzahl von Standards und bieten vielfältige Möglichkeiten für Überwachungen und Benachrichtungen bei kritischen Situationen. Die Stabilität der Appliances ist beeindruckend, und sie ermöglichen es uns, den laufenden Betrieb noch besser zu überwachen.“ Das Fazit lautet: „Nach unserer Überzeugung ist es äußerst sinnvoll, robuste, durchsatzfähige und spezialisierte Geräte für die Sicherheit im Bereich Webservices einzusetzen, besonders für uns als Finanzdienstleister mit hohem Anspruch an die Sicherheit. Die IBM DataPower Appliances passen einfach.“

Weitere Informationen

Wenn Sie mehr über IBM WebSphere DataPower SOA Appliances erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

ibm.com/software/de/websphere/integration/datapower.html

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in Deutschland 03/2011.

Die IBM Homepage finden Sie unter:
ibm.com

Bitte recyclen

WebSphere software