

Security eröffnet neue Möglichkeiten

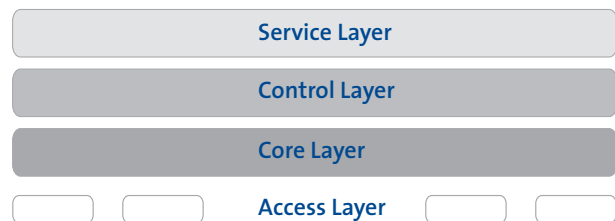
SICHERE WEB SERVICES ALS UNIVERSELLE PLATFORM BEI O₂

Der Telekommunikationsbranche eröffnen sich durch Web Services weitreichende Möglichkeiten, ihren Kunden komfortablere Dienste anzubieten und die eigenen Geschäftsprozesse zu optimieren. Die damit verbundenen Kostenvorteile und Umsatzsteigerungen zu realisieren, ist auch das Ziel des Mobilfunkbetreibers O₂ Germany. Einer uneingeschränkten Nutzung von Web Services stehen bei O₂ allerdings die branchenüblich hohen Sicherheitsanforderungen gegenüber. Durch den Einsatz der Xtradyne-Sicherheitstechnologien konnte diesen Anforderungen entsprochen werden, so dass sich diese Web Services nun einsetzen lassen.

Heutige (und erst recht künftige) Telekommunikationsnetze sind universelle Plattformen für eine große, heute noch kaum absehbare Anzahl von Diensten. Beispiele für aktuelle Dienste für Mobilfunknetze sind MMS-Benachrichtigungen oder Anwendungen, mit denen Großkunden ihre Dienstenutzung selbst konfigurieren und anpassen können.

Erst durch die Öffnung der Netze und die Integration von Diensten wird es möglich, das volle Potential der vorhandenen Infrastruktur zu nutzen und überall verfügbare Dienste anzubieten. Dabei verschwimmen die Grenzen zwischen klassischen, knotenbasierten Fernmeldediensten und IN- oder IT-gestützten Mehrwertdiensten immer mehr.

Der Markt für innovative Telekommunikationsangebote, speziell der Mobilfunkmarkt, erfordert eine extrem hohe Flexibilität und sehr kurze Zeiten bis zur Markteinführung, um als erster durch strategische neue Produkte auch neue Kundengruppen ansprechen zu können. Telekommunikationsanbieter müssen daher möglichst schnell und einfach neue Dienstbausteine und Anwendungen mit vorhandenen kombinieren und integrieren können und dabei auch auf die Nutzung externer Komponenten und den Weiterverkauf von Diensten externer Anbieter vorbereitet sein. Den Investitionen in die Entwicklung und Etablierung flexibler, dienstorientierter Architekturen (SOA, Service Oriented Architecture), die heterogene Plattformen und Technologien der eigenen Netze zu einer Dienstschicht vereinheitlichen, kommt damit eine unternehmensstrategische Bedeutung zu.



Dienstschicht und Netzschichten

XML Web Services

XML Web Services ermöglichen eine dienstbezogene Sicht auf vorhandene Technologie und sind ein Eckpfeiler von SOAs. Web Services ermöglichen eine einfache und schnelle Integration vorhandener Plattformen und Anwendungen und bieten daher genau den strategischen Vorteil, der in dynamischen Märkten wie dem Mobilfunkmarkt entscheidend ist.

Daher sind Web Services bei innovativen Anbietern wie O₂ bereits seit einiger Zeit in der Entwicklung. Web Services basieren intern auf dem Austausch bestimmter XML-Dokumente (SOAP-Nachrichten) zwischen Anwendungen, wobei diese Nachrichten interne oder sogar externe Netzgrenzen durchqueren müssen.

Solche Kommunikation unterliegt bei O₂ den in der Telekommunikationsbranche üblichen, strengen Sicherheitsrichtlinien. Die Richtlinien von O₂ schlossen insbesondere einen sofortigen und uneingeschränkten Einsatz von SOAP zunächst gänzlich aus:

„SOAP-Nachrichten können von einer Firewall nicht kontrolliert werden (Tunnelling, Content Inspection), so dass ein Einsatz über Netzsegmente hinweg aus Sicherheitssicht nicht akzeptabel ist. Daher ist unkontrollierter netzübergreifender SOAP-Verkehr bei uns grundsätzlich ausgeschlossen“, so Frank Zabawa (Corporate Security) und Dr. Jörg Schreck (Service Management-Security) von O₂.

Security für Web Services

Um dennoch wie geplant Web Services-basierte Dienste anbieten zu können, stellte sich O2 schon früh die Frage nach geeigneten Sicherheitsmechanismen, mit denen die firmeneigenen Sicherheitspolitiken eingehalten werden können. Neben der Authentisierung von Nachrichten sind dafür vor allem eine flexible Autorisierung und die Abwehr schädlicher Inhalte in SOAP-Nachrichten notwendig, und das bei sehr hohen Durchsatz- und Verfügbarkeitsanforderungen.



Sicherheit im Service Layer

Da diese Anwendungssicherheit von keinem der herkömmlichen Firewalls erbracht wird, begann O2 einen mehrmonatigen Auswahlprozess für spezielle SOAP-Firewall-Produkte, in dem sich der Xtradyne Web Services Domain Boundary Controller (WS-DBC) von Xtradyne durchsetzte, PrismTechs Security-Produktlinie. Der WS-DBC ist ein Sicherheitsgateway, das SOAP-Nachrichten transparent diversen Sicherheitsprüfungen unterzieht, bevor diese weitergeleitet werden. Darüberhinaus ermöglicht er ein einheitliches Sicherheitsmanagement über Plattformgrenzen hinweg.

„Der WS-DBC erlaubt es, unseren Anwendungsverkehr direkt und ohne jede Modifikation der Anwendungen abzusichern, so dass wir nicht länger auf den Einsatz in Back-end-Netzen beschränkt sind“, so Dr. Mathijs Dijkhuizen, Projektleiter bei O2 Germany. *„Unsere Web Service-Projekte konnten daher ohne Verzögerung an den Start gehen.“*

O2 macht dabei ausgiebigen Gebrauch von den fortgeschrittenen Möglichkeiten der Inhaltsfilterung, die der WS-DBC bietet. Durch XPath-Filter und XML Schema-Validierung werden dabei etwa die Datentypen und Inhalte ein- und ausgehender Nachrichten geprüft, um z.B. das Eindringen potentiell schadenbringender Inhalte zu verhindern, die etwa in der Form von Buffer Overflow attacks möglicherweise auftretende Schwachpunkte in Implementierungen ausnutzen könnten.

Außerdem wird der WS-DBC in den Hochverfügbarkeitsszenarien betrieben, die für die Telekommunikationsbranche typisch sind. „Der WS-DBC bietet uns genau die Lastverteilungs- und Mehrprozessorunterstützung, die wir brauchen“, so Dirk Schoob, Master Specialist IN im Network Competence Center von O2. *„Durch die rein software-basierte Architektur sind wir zudem extrem flexibel beim Deployment.“*



PrismTech (Deutschland) GmbH
Xtradyne Security Technologies
Öffentlichkeitsarbeit
Schönhauser Allee 6-7
D-10119 Berlin

Tel. +49-30-440 306-18
Fax +49-30-440 306-78

Email: info@xtradyne.de
Internet: www.xtradyne.de