Webservices fordern ein neues Sicherheitsdenken

Orbit/Comdex 2003

Webservices fordern ein neues Sicherheitsdenken

IT-Security ist heute eines der wichtigsten Themen der Informationstechnologie. Daran wird sich auch in Zukunft nichts ändern. Im Gegenteil: Mit der Einführung von Webservices, dem nächsten Evolutionsschritt des World Wide Web, wird die Bedeutung der Informationssicherheit nochmals deutlich zunehmen. Die Sicherheitsbranche wird auch in Zukunft mit einem überdurchschnittlichen Wachstum rechnen können.

IT-Security» war an der Orbit/Comdex 2003 vom 24. bis 27. September in Basel ein Schwerpunktthema.

Das übersichtliche Web, ein Traum?
Tim Berners-Lee, der Erfinder des World Wide Web, ist besessen von einer fixen Idee: Er möchte das Internet entrümpeln, um so den Benutzern die Suche nach gezielten Informationen so einfach wie möglich zu machen. Dem WWW-Erfinder und Vordenker des internationalen World-Wide-Web-Konsortiums (W3C) schwebt ein intelligentes, «semantisches Web» vor, in dem es keine ungeordneten Text- und Bilderhalden mehr gibt, die von Suchrobotern durchforstet werden müssen. Stattdessen sind alle wesentlichen Informationen einer Webseite mit Angaben zu ihrer Bedeutung versehen – daher auch die Bezeichnung semantisch (von griechisch «sem» für Bedeutung). Doch nicht nur Informationen sollen für jeden einfach auffindbar werden, sondern auch Applikationen und Dienste, eben auch Services.
Und hier spätestens beginnt das Problem: Damit Berners-Lees Vision überhaupt verwirklicht werden kann, braucht es umfassende und hochkomplexe Sicherheitsmechanismen. Die besonderen Sicherheitsanforderungen erklären sich durch den Umstand, dass Webservices in sich abgeschlossene und selbstbeschreibende modulare Applikationen darstellen, die über das Internet veröffentlicht, lokalisiert und aufgerufen werden können. Sie führen Funktionen aus, die von einfachen Abfragen bis hin zu komplexen Geschäftsanwendungen reichen können. Dabei können die einzelnen Software-Module unabhängig von der darunter laufenden Plattform eingesetzt werden. Ein Grossteil der Kommunikation findet ausserdem mehr oder weniger automatisch zwischen verschiedenen Rechnern oder Anwendungen statt; dies im Unterschied zum bisherigen Modell, das auf einer starken Einbindung des Menschen beruht. Bei Webservices sind Menschen nur noch in vergleichsweise wenigen Transaktionen direkt involviert. Hinzu kommt, dass sich ein Webservice nahezu überall befinden kann, also auch in einer Umgebung, deren Sicherheitsanforderungen unter Umständen nicht sehr hoch sind.

Neues Sicherheitsdenken gefragt
Webservices bewegen sich in einem komplexen und wenig übersichtlichen Raum. Damit überhaupt geschäftskritische Abläufe abgebildet werden können, bedarf es eines hohen Masses an Sicherheit. Im Vordergrund stehen dabei die Integrität und die Authentizität übertragener Informationen sowie die Vertraulichkeit von Transaktionen. Diese müssen gewahrt bleiben, damit Inhalte nicht manipuliert oder gefälscht werden können. Ausserdem sind eine Überprüfung der Identität und eine Autorisierung der Webservices-Einheiten notwendig. Ebenfalls wichtig für die Sicherheit von Webservices ist die Verbindlichkeit oder Unabstreitbarkeit (Non-Repudiation). Es muss sichergestellt werden, dass niemand, der eine Transaktion durchgeführt hat, dies im Nachhinein abstreiten kann. Im WWW gibt es zwar Techniken, die für Sicherheit sorgen, wie etwa das Protokoll Secure Sockets Layer (SSL), das häufig bei Banken für den sicheren Online-Zugriff auf Konten eingesetzt wird. Doch die bestens erprobte Technik SSL lässt sich mit Webservices nur sehr schlecht einsetzen, da sie den kompletten Datenstrom verschlüsselt und somit wichtige Routing-Informationen, die mit Hilfe des Simple Object Access Protocol (Soap) ebenfalls übertragen werden, nicht mehr ausgelesen werden können.
Da Webservices selbst keine Sicherheitsmechanismen vorsehen, sind verschiedene Gremien derzeit damit beschäftigt, auf Basis der Extensible Markup Language (XML), die sich zum De-facto-Standard für Webservices entwickelt hat, Erweiterungen zu definieren, welche die Schwachstellen ausräumen sollen.

Ohne digitalen Ausweis geht nichts
Beispielsweise die von der Organisation for the Advancement of Structured Infor-

mation Standards (Oasis) verabschiedete Spezifikation Security Assertions Markup Language (SAML). Sie stellt eine Möglichkeit für Webservices dar, sich gegenseitig zu identifizieren und Informationen bezüglich ihrer Authentizität auszutauschen. Das geschieht in Form so genannter Security Assertions, die Anwendern, Applikationen oder einem Webservice zugewiesen und in speziellen Verzeichnissen vorgehalten werden können.
Mit SAML lassen sich so genannte Single-Sign-on-Systeme realisieren. Folgender Gedanke steckt dahinter: Nach einmaligem Anmelden an einem System kann der Nutzer auf weitere, damit verbundene Dienste zugreifen, ohne sich erneut anmelden zu müssen. Die SAML-Spezifikation bildet die Grundlage für die Arbeit der von Industrierepräsentanten wie Sun, Cisco und RSA Security initiierten Liberty Alliance, die sich zum Ziel gesetzt hat, eine herstellerneutrale, offene Lösung für digitale Identitätsausweise zu erarbeiten.
Ein ähnliches Ziel verfolgen Microsoft und IBM mit der Global XML Web Services Architecture (GXA). Diese setzt auf dem von beiden Unternehmen gemeinsam mit der US-Sicherheitsfirma Verisign entworfenen Sicherheitskonzept WS-Security auf, das ebenfalls zur Standardisierung an Oasis weitergeleitet wurde. WS-Security erweitert Soap um Funktionen wie Verschlüsselung und digitale Signaturen. IBM und Microsoft sehen ihre Lösung nicht als Ersatz von SAML, sondern als Erweiterung.
An einem weiteren Standard arbeiten das World-Wide-Web-Konsortium (W3C) und Internet Engineering Task Force (IETF). Dabei handelt es sich um die XML Key Management Specification (XKMS). Sie beschreibt Protokolle für das Erzeugen, Verteilen und Registrieren von öffentlichen Schlüsseln. XKMS stellt eine Art Public-Key-Infrastruktur (PKI) für Webservices zur Verfügung.

Herkömmliche Firewalls taugen nichts

Webservices bedingen nicht nur ein neues Sicherheitsdenken in den Unternehmen, sie stellen auch die Hersteller von Firewalls vor ganz neue Herausforderungen. Derzeit können nämlich diese Brandschutzmauern für Unternehmensdaten nur so konfiguriert werden, dass sie Soap-Messages entweder durchlassen oder vollständig abblocken. Künftig werden Webservices aber über die Grenzen von Unternehmensnetzen hinweg miteinander kommunizieren. Deshalb müssen Firewalls in Zukunft «lernen», Soap-Messages zu interpretieren, um von Fall zu Fall selbstständig entscheiden zu können, ob die Message zulässig ist oder nicht.
Den Sicherheitsexperten schwebt hier eine separate Sicherheitslösung vor, die analog zur Firewall eine Pförtnerrolle wahrnimmt und zwischen einer vertrauten Umgebung und einer unsicheren Zone vermittelt. So ist es denkbar, dass eine bestimmte Gruppe von Webservices untereinander mit relativ geringer Sicherheit kommunizieren kann. Das geschieht typischerweise innerhalb eines Unternehmensnetzes. Doch sobald diese die vertraute Zone verlassen, greift die Sicherheitskomponente ein und führt auf Basis definierter Regeln Schutzvorkehrungen durch.

Es gibt noch viel zu tun

Die vorgeschlagenen Ansätze und Konzepte zur sicheren Verteilung und Nutzung von Webservices machen überdeutlich, dass der Industrie viel an diesem Thema liegt und mit Hochdruck an der Entwicklung von Sicherheitslösungen gearbeitet wird. Vieles indessen, das jetzt noch sehr kompliziert klingt, wird in Zukunft einfacher werden müssen, damit die Anwender sich überhaupt zurechtfinden werden. 12