Computerworld Technologie & Service

Inhalt

Lexikon

Choreography

Datenaustausch auf Basis von XML (Extensible Markup Language) und Soap (Simple Object Access Protocol) hat sich im Geschäftsbereich als künftiges Paradigma fest etabliert. Die beiden gut eingeführten Protokolle decken aber noch nicht das ganze Spektrum an Regeln ab, die zwischen Geschäftspartnern definiert werden müssen. Zum einen müssen sich das Format und die Struktur von Botschaften, die auf Basis von Soap ausgetauscht werden, genauer bestimmen lassen, zum andern müssen auch die Reihenfolge eines Datentausches und die Bedingungen für einen solchen genau festgelegt sein.

Das erstere leistet WSDL (Web Services Definition Language), das zweite ist Thema von zwei konkurrierenden Standards: Zum einen haben Microsoft, IBM und BEA mit BPEL4WS eine Spezifikation für die Erledigung dieser Aufgaben entwickelt und im April 2003 beim Standardisierungsgremium Oasis (Organisation for the Advancement of Structured Information Standards) eingereicht. Beim W3C (World Wide Web Consortium) wird auf der andern Seite an der Web Services Choreography getüftelt, die dasselbe leisten soll. Die Choreography des Konsortiums wird in drei Varianten ausformuliert, einer abstrakten, einer konkreten und einer portablen. Eine abstrakte Choreography ist eine Art Schablone in der die konkrete Struktur einer Botschaft nicht festgelegt ist. Ebenfalls offen bleibt die zu nutzende Technologie. Werden Technologie und Struktur der Botschaft definiert, wird die abstrakte zu einer portablen Choreography.
Die unnötigen Doppelspurigkeiten von Web Services Choreography und BPEL4WS sollen vermieden werden. Interessenvertreter beider Gruppen haben sich an einen Tisch gesetzt und über eine mögliche Kooperation debattiert. Im März rief Oasis das technische Komitee «Web Services Reliable Messaging» ins Leben, das sich zusätzlich dem Problem des Messaging annehmen soll. *wb*

IT-Sicherheit in der Kostenfalle

Security-Offerten Schweizer IT-Spezialisten gehen davon aus, dass nur etwa 20 Prozent des Schadens, den Firmen durch den Einsatz von IT-Techniken erleiden, auf die eingesetzte Hard- und Software entfallen. 80 Prozent der Kosten sind auf organisatorische Mängel zurückzuführen.

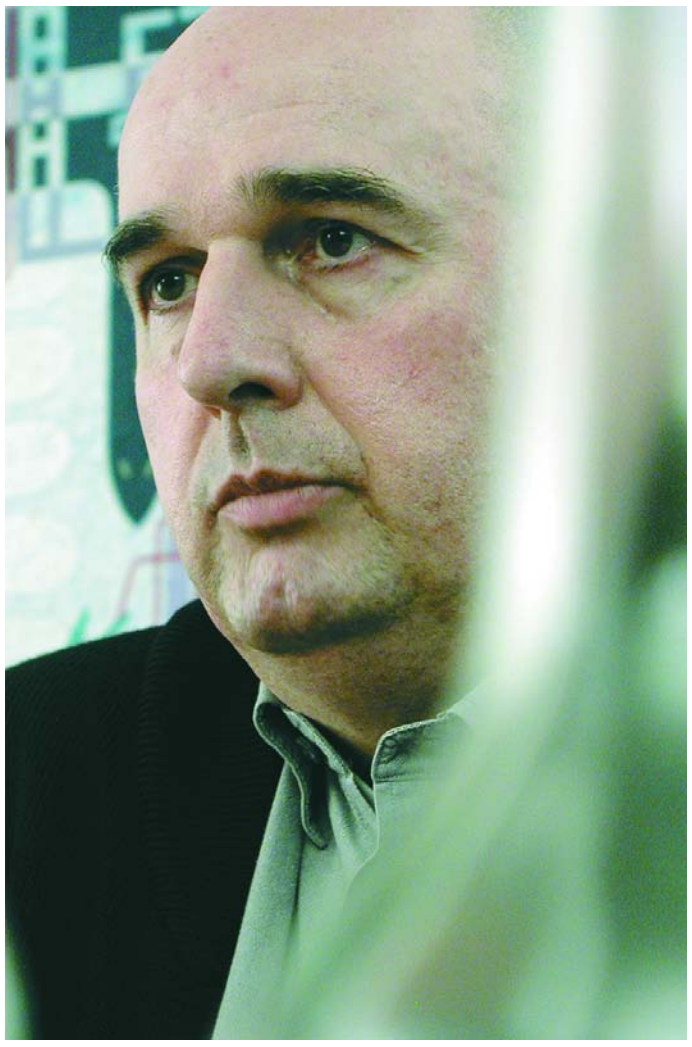
Volker Richert

Wer die Struktur, das Konzept und die Vergleichbarkeit von Offerten für die IT-Sicherheit befragt, trifft immer wieder auf ein ziemliches Durcheinander. Allein schon der Versuch, den Begriff IT-Sicherheit einzugrenzen, führt von «ganz individuellen» und nach Aufwand bezahlbaren bis zu «prozessorientierten» und aufgrund des Umsatzes bezifferbaren Sicherheitsvarianten. Sicher ist in Sachen IT-Security dabei offensichtlich nur, dass sich das komplexe Thema und die Vergleichbarkeit der Angebote ausschliessen.

Standard für Offerten

IT-Berater Felix Widmer von der Tan Consulting in Rapperswil bestätigt diese zum Abzocken einladende Offertsituation. Für ein Sicherheitsbudget, so Widmer lassen sich dennoch klare Zahlen angeben, die in der Regel bei rund 20 Prozent des Informatikbudgets liegen. Auf Security-spezifische Hard- respektive Software und Infrastrukturmassnahmen entfallen davon etwa 20 Prozent; das sind nur vier Prozent aller IT-Kosten.

Was über diese Aufwendungen hinausgeht, Widmer spricht von «weichen Faktoren» und meint die Beratung, ist aber viel schwieriger in Zahlen zu fassen. Und das, obwohl es sich immerhin um 80 Prozent der Security-Kosten handelt. Um diesbezüglich nicht in eine Grauzone abzurutschen, empfiehlt Widmer den Rückgriff auf Normen und Standards. Sie können von der Analyse bis zur Angebotsstellung Leitplanken bilden.



Felix Widmer: «Standards verhelfen zu transparenten Offerten.» Foto: CW/gis

Dass besonders im KMU-Bereich die Probleme in der Regel schon mit der Definition eines Soll-Zustands beginnen, streitet Widmer nicht ab. Denn den Kunden fehlt oft die Kompetenz für diese Grundlagenbestimmung. «Aber deshalb haben die IT-Berater ja gerade ihre Berechtigung», meint Widmer. Der Widerspruch von Standardisierung und Beraterabhängigkeit fordert hier einen Spagat: «Transparentes Vorgehen bei der Offertstellung», nennt der Berater den Ausweg. Einen anderen Weg, Widersprüchen zu begegnen und auf umsatzabhängige Offertstellungen zu setzen, wie das der Riskoanalyst Artur Schmidt von der Immunologix in Basel für KMU und Grossfirmen empfiehlt, lehnt Widmer dagegen als «wenig seriös» ab. Fragt sich also, wie man konkret zu einer vergleichbaren Offerte kommt. Auch Widmer analysiert anfangs die Geschäftsprozesse, zieht dabei aber konsequent Hilfestellung zu Rate wie «Code of Practice for IT Security Management» (BS 7799 beziehungsweise ISO 17799).

Security by Objectives

Anhand solcher Regelwerke lässt sich laut Widmer eine Adaption an jeweils anstehende Projekte durchführen: «Zu dessen Ausarbeitung muss der Berater nebst organisatorischem und betriebswirtschaftlichem Wissen gute Kenntnisse der ITIL-Methode (Information Technology Infrastructure Library) und des IT-Grundschutzhandbuches mitbringen.» Um von Anfang an gegenüber der Revision transparent und nachvollziehbar zu sein, sind zudem die Anforderungen von COBIT (Control Objectives for Information and Related Technology) zu berücksichtigen. Anhand dieser Standards erstellt Widmer eine Checkliste, womit er die IT-Sicherheit von den Zielsetzungen her definieren und umsetzen kann. «Vergleichbarkeit ist gewährleistet, weil jeder andere Security-Anbieter auf diese Ergebnisse aufsetzen kann.» Klar sein muss laut Widmer, «Informatik ist nur ein unterstützender Prozess, im Zentrum steht der Geschäftsprozess. Security liegt immer in der Verantwortung des Top-Managements».

Offerte sauber berechnen

Widmer empfiehlt die Angebotsstellung in vier Schritten: 1. In einem halben Arbeitstag werden mit der Geschäftsleitung die Anforderungen der Geschäftsprozesse definiert. 2. Ein erfahrener Berater kann diese Ergebnisse in zwei Tagen Schreibtischarbeit zur Struktur der IT-Security für das Unternehmen anhand von Standards ausbauen. 3. In einem Tag mit den IT-Verantwortlichen werden anhand dieses Grobkonzepts messbare Zielsetzungen definiert. 4. Detailliert legt der Berater in weiteren zwei Tagen Büroarbeit das Regelwerk mit Sicherheits-Leitbild, Schutzbedarfsfeststellung und Sicherheitsprozess vor. Nun kann die Umsetzung ausgeschrieben werden. Widmer spricht von einem «Framework», als Grundlage zur Ausführung, die nun präzise beziffert werden kann. Die Framework-Kosten seien überschaubar. Ausserdem würde das Framework in der Realisierung einer praktischen Prüfung unterzogen. «Abzockerei sei auf diese Weise gewiss nicht möglich,» sagt der Berater.

Transparenz

Aus Erfahrung weiss der Berater natürlich, dass wer sich den Auftrag fürs Regelwerk schnappt, meist auch Folgearbeiten erhält. Dennoch betont Widmer standardsorientierte Transparenz. IT-Security-Wissen darf nicht zu Abhängigkeiten führen. Widmer ist optimistisch: «Bedrohungen werden heute gern aufgebauscht». Er befürchtet allerdings eine IT-Security, die zum Experimentierfeld der Spezialisten verkommen ist. «Sicherheit kann und soll einfach gestaltet werden. Dazu brauchts wieder mehr gesunden Menschenverstand.»

Info/http://www.tan-group.ch

IT-Sicherheit ist zertifizierbar

Das vernünftige Vorgehen von der Einführung über die Implementation bis zum Unterhalt der IT-Sicherheit in Unternehmen oder Organisationen beschreiben die ISO 17799 und BS 7799-2. Diese Normen bieten Definitionen und Spezifikationen und helfen bei der Entwicklung eigener, anwenderorientierter Regeln und Praktiken für die IT-Security. Ausserdem lässt sich anhand dieser Standards die Einhaltung rechtlicher Pflichten genauso wie die internen Anforderungen zur IT-Sicherheit überwachen. Der in der ISO 17799 enthaltene Leitfaden zur Steuerung der IT-Sicherheit bietet sich zudem als ein formal möglicher Weg zur Zertifizierung eines IT-Sicherheits-Managementsystems nach BS 7799-2 an.

Info/http://www.iso.org

ITIL beschreibt IT-Prozesse

ITIL (Information Technology Infrastructure Library) definiert als «Best Practice Framework» IT-Prozesse und deren Betrieb. ITIL ist eine allgemein zugängliche Bibliothek, die von der englischen Behörde OGC (Office of Government Commerce) entwickelt wurde. Inzwischen liegen 40 Bücher vor, in denen die zur Zeit wichtigsten IT-Prozesse beschrieben sein sollen. Diese Sammlung von Literatur wird heute als Baukasten für das IT-Service-Management verstanden, ein Referenzsystem mit kundenorientierter Ausprägung der Prozesse. ITIL ist erweiterbar um Prozesse, die nicht ursprünglich zum IT-Service-Management zählen. Implementiert wird es als Bestandteil des Qualitätsmanagements.

Info/http://www.itil.org

Ein Katalog an Massnahmen

Vom IT-Grundschutzhandbuch des deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik) liegt eine soeben erst aktualisierte Version vor. Geboten werden Hilfestellungen bei der Analyse und Bewertung der IT-Sicherheit sowie bei der kontinuierlichen Umsetzung von alltäglichen Standard-Sicherheitsmassnahmen. Zudem wird der Prozess zur Erkennung und Beseitigung von Defiziten in der Security-Infrastruktur beschrieben. Dazu gibts in dem Handbuch jede Menge Sicherheitskriterien, mit konkreten Vorschlägen zur Lösung von Sicherheitsproblemen und der Beschreibung des entsprechenden methodischen Vorgehens. Soll- und Ist-Zustand der IT-Sicherheit lassen sich damit definieren.

Info/http://www.bsi.de