

Hohe Erwartungen

Security ■ Die Sicherheit von IT-Lösungen ist und bleibt speziell in der Finanzdienstleistungsbranche ein brennendes Thema. Die Probleme und auch die Lösungsansätze sind bekannt. Die aktuelle Herausforderung besteht darin, aus den einzelnen Bauteilen ein Gesamtsystem zu schaffen.

Wie auch in anderen Bereichen der IT wird im Sicherheitsbereich vermehrt auf Standards gesetzt. Denn der Einbau von proprietären Sicherheitslösungen widerspricht eigentlich dem Gedanken der Sicherheit.

KARIN BOSSHARD

«**SCHWEIZER BANK**»: Weshalb ziehen Sie die standardisierten den proprietären Lösungen vor? Sind diese in jedem Fall besser?

Stefan Wengi: So absolut würde ich das nicht sagen. Speziell im Sicherheitsbereich gilt es, auf Grund der Kundenbedürfnisse und der «Best Practice»-Erfahrungen die optimale Lösung zu vertretbaren Kosten zu finden. Dabei kann der Einsatz bereits bestehender proprietärer Komponenten durchaus sinnvoll und auch in sicherheitstechnischer Hinsicht richtig sein. Grundsätzlich tendieren wir aber schon zu offenen Standards und halten wenig von «Security by Obscurity».

Für den Einsatz von offenen Standards wie J2EE Security oder SSL spricht unter anderem die breite Unterstützung durch namhafte Gremien und Unternehmen sowie die im Umfeld einer Spezifikation geführte offene Diskussion unter Experten. Offene Standards gewährleisten die Tauglichkeit und Überprüfbarkeit der eingesetzten Verfahren und die optimale Interoperabilität und Herstellerunabhängigkeit.

«**SB**»: Welche Rolle spielt Open Source Software in der Security?

Wengi: Speziell für hochsichere Komponenten sind Open-Source-Produkte eine gute Wahl, denn hier kommen die Vorteile offener Standards auf einer zusätzlichen Ebene zum Tragen. Nicht nur die eingesetzten Verfahren, sondern auch ihre Implementierung ist prüfbar. In der AdNovum spielen Open-Source-Produkte deshalb seit jeher eine tragende Rolle. Um eine volle Transparenz zu gewährleisten, sollte immer der gesamte Programmcode mitgeliefert werden. Der Kunde hat damit die Möglichkeit, eigene Verifikationen durchzuführen.

«**SB**»: Worin besteht die grösste Herausforderung bei der Schaffung eines funktionierenden Gesamt-Sicherheitssystems? Welche Besonderheiten müssen dabei bei Finanzinstituten berücksichtigt werden?

Wengi: Die grösste Herausforderung liegt ganz klar in der Definition der notwendigen betriebsorganisatorischen Abläufe und in der Mitarbeitersensibilisierung. Die Vorstellung, mit dem Kauf eines Produkts von der Stange sei der Security Genüge getan, erweist sich als gefährliche Illusion, vor allem im anspruchsvollen Finanzumfeld. Die Einhaltung von Security-Richtlinien in Bereichen wie Zertifikatsmanagement und Audit ist sehr wichtig, ebenso die regelmässige Durchführung interner und externer Security Reviews. Zusätzlich sind Integrations- und Sicherheitstests beim Kunden erforderlich. Auf der rein technischen Seite besteht die grösste Herausforderung

darin, die einzelnen Softwarebauteile, inklusive Middleware, zu einem hochsicheren Gesamtsystem zusammenzuführen.

«**SB**»: Was verstehen Sie unter High-Grade Security?

Wengi: Hochsichere Systeme setzen sich aus einzelnen Komponenten zusammen. Damit das System als Ganzes sicher ist, müssen alle beteiligten Kom-

Stefan Wengi, diplomierter Informatik-Ingenieur ETH, ist CTO des Zürcher Software-Unternehmens AdNovum Informatik AG. Sein Schwerpunktthema ist Technology/Middleware.



ponenten auf allen Ebenen sicher sein. Zentrale Anforderungen sind dabei die sorgfältige Programmierung gemäss anerkannten Richtlinien, die Verwendung von Schlüsseln von mindestens 128 Bit Länge, der konsequente Einsatz von Stan-

dardschnittstellen wie PKCS #11 und GSSv2, die Speicherung von Schlüsseln auf einer manipulationssicheren Hardware, die Einrichtung dedizierter Sicherheitszonen, der Schutz des Internetzugriffs über einen Reverse Proxy sowie eine sichere Propagation der Identität über alle an der Kommunikation beteiligten Knoten.

«**SB**»: Welche Faktoren haben dazu beigetragen, dass es zurzeit keine offizielle Zertifizierungsstelle in der Schweiz gibt? Wie beeinflusst dies Ihre Arbeit?

Wengi: Ausschlaggebend waren primär die hohen Investitions- und Betriebskosten auf Seiten des Dienstleistungsanbieters. Auf unsere Arbeit hat das Fehlen einer offiziellen Stelle keinen direkten Einfluss, da wir eine eigene Certificate Authority unterhalten. Die Arbeit unserer Kunden allerdings wird durch den aktuell unsicheren Stand sicher beeinträchtigt. Der Ruf nach einer vertrauenswürdigen Zertifizierungsstelle auf Schweizer Boden und nach Schweizer Recht ist gerechtfertigt. ■

Neue Zertifizierungsstelle in der Schweiz?

«Eine neue gesamtschweizerische Zertifizierungsstelle sollte von einer öffentlich-rechtlichen Instanz geführt und betrieben werden», erklärt Stefan Wengi. «Nahe liegend wäre der Bund oder ein bundesnahes Unternehmen. Es existieren auch Anstrengungen und Verrechnungsmodelle, um die Kosten anders als durch den Verkauf von Zertifikaten abzugelten. Eine Zertifizierungsstelle könnte somit durchaus Gewinn bringend unterhalten werden. Die technischen Voraussetzungen sind dabei weniger das Thema, wie wir auf Grund der von uns gebauten Public-Key-Infrastrukturen bestätigen können. Vielmehr geht es um die Formulierung von Bedürfnissen und um politische Entscheide.»