

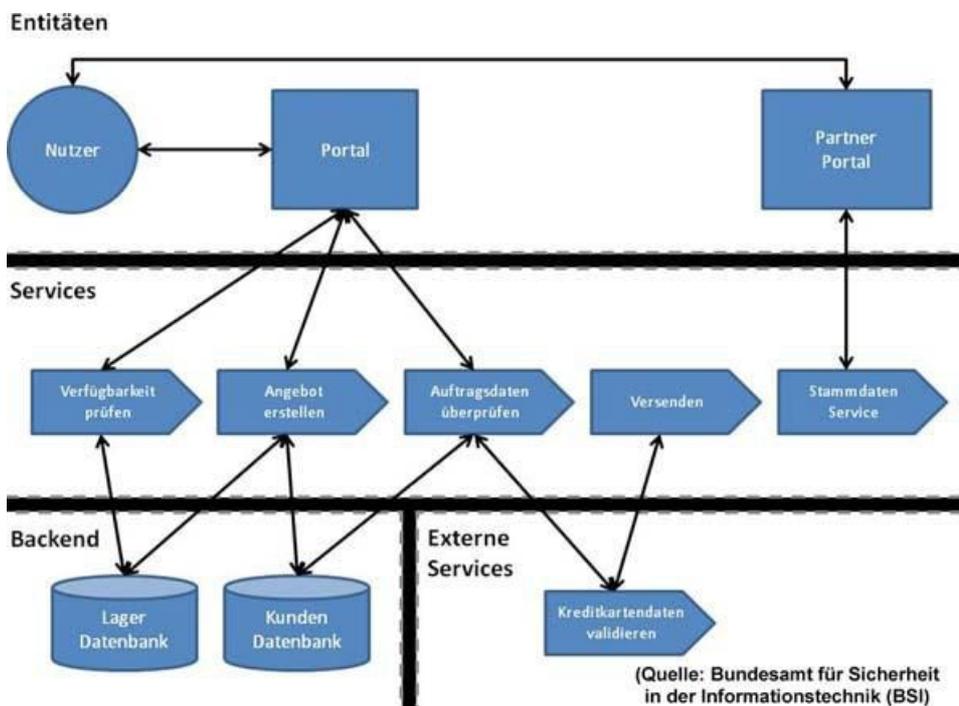
Link: <https://www.computerwoche.de/a/soa-macht-unternehmensnetze-unsicher,1882007>

Security-Kompodium des BSI

## SOA macht Unternehmensnetze unsicher

Datum: 16.12.2008  
Autor(en): Andreas Schaffry

**Service-orientierten Architekturen (SOA) umfassen meist kritische und daher besonders schutzbedürftige Geschäftsprozesse in Unternehmen. Sowohl für die Sicherheit einzelner Service-Anfragen in Bezug auf Vertraulichkeit, Authentizität oder Autorisierung als auch für die Sicherheit von Transaktionen müssen entsprechende Vorkehrungen getroffen werden.**



Das BSI stellt im "SOA Security Kompodium" die wichtigsten Konzeptionen zur Absicherung einer SOA vor. Hier: Die Verläufe der Daten im Unternehmen. Quelle: BSI, 2008

Durch die Implementierung einer SOA öffnen Unternehmen ihre Prozesse sowie die dahinter liegende Geschäftslogik gegenüber Kunden und Partnern. Dabei beachten Unternehmen bisher kaum, dass von der Öffnung nach außen auch interne Geschäftsprozesse betroffen sind und die Sicherheitsanforderungen deutlich steigen.

In SOA-basierten IT-Landschaften sind neben der Sicherheit einzelner Service-Anfragen, etwa im Hinblick auf Vertraulichkeit und Authentizität, auch Aspekte wie Transaktions-Sicherheit von Bedeutung.

### Neue Bedrohungspotentiale

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich mit der Sicherheit in SOA-basierten IT-Umgebungen auseinandergesetzt und stellt im "SOA-Security-Kompodium" die wichtigsten Konzeptionen und Technologien zur Absicherung Service-orientierter IT-Architekturen vor. Darüber hinaus zeigen die BSI-Experten, wie sich Sicherheit in einer SOA-Infrastruktur konkret umsetzen lässt.

Die Bedrohungspotentiale in einer SOA decken sich zwar teilweise mit denen konventioneller IT-Systeme. Der klassische Sicherheitsansatz, nur die Ränder des Informationssystems zu schützen, greift jedoch in Service-basierten IT-Landschaften zu kurz, da diese nicht klar definiert sind. Als SOA-spezifische Bedrohungspotenziale gelten Replay-Angriffe, XML-spezifische Angriffe, WSDL- und Service-Scanning, die Kompromittierung von Services, unberechtigte Service-Nutzung und Ausnutzung von Organisationsschwächen.

Bei der Absicherung einer SOA sind zudem spezifische Besonderheiten, wie etwa die Problematik verteilter Strukturen sowie Administrations- und Beherrschbarkeitsaspekte, zu berücksichtigen. Geschäftsprozesse, die lose über Services gekoppelt sind, erfordern mehr Authentisierungsvorgänge, zudem muss die Vertraulichkeit und Integrität des Informationsaustausches jederzeit gewährleistet sein.

Als weitere sicherheitsrelevante Aspekte beim Aufbau einer SOA identifizieren die BSI-Experten die Themen Autorisierung, Verbindlichkeit, Verfügbarkeit und Ausfallsicherheit, Administrierbarkeit sowie Datenschutz und Audit.