12. Mai 2016 Studie · Web & Cloud

# Sicherheitsmanagement von API-basiertem Datenaustausch

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

**Archiviert.** Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

**Quelle** https://technology2.a-sit.at/veroeffentlichungen/benutzerzentriertes-sicherheitsmanagement-von-api-basierten-datenaustausche/

Sicherheitsanforderungen – insbesondere jene zur Vertraulichkeit – erfordern IT-Prozesse mit dem Least-Privilege-Prinzip. Das aktuell breit verwendete Autorisierungsprotokoll OAuth 2.0 entspricht diesen Anforderungen nur teilweise. Etwa entfällt wegen frei definierbarer und dienstleisterabhängiger Darstellung von Access-Scopes praktisch die Möglichkeit, die Zugriffsbeschränkungen und -Autorisierungen strukturiert, granular und interoperabel darzustellen. Dieses Problem betrifft insbesondere domänenübergreifenden Datenaustausch, da die Sicherheitsmaßnahmen in verschiedenen Organisationen nur teilweise angewandt werden können.

Die Architektur sowie die einschlägige Ergebnisse wurden im Rahmen des DISSECT Workshops bei der IEEE/IFIP NOMS Konferenz präsentiert. Der vorgeschlagene Ansatz behandelt das Sicherheitsmanagement von API Interaktionen. Die Perspektiven von Dienstanbietern, Klienten und Dateninhaber werden in betrachtet, um die kontextuelle Abhängigkeit bei Datenaustausch, sowie die Granularität und Interoperabilität bei Sicherheitsmanagementprozessen, zu ermöglichen.