Bundesministerium
für Wirtschaft
und Technologie

Trusted Cloud

Presseinformation

MimoSecco

Vertrauensvolles Datenmanagement für Cloud-Dienste

Unternehmensdaten in der Cloud müssen gut geschützt sein. Erprobtes Mittel dazu ist eine ausreichende Verschlüsselung der Daten bei Transport und Speicherung. Sollen diese Daten allerdings vom Anwender bearbeitet werden, müssen sie zumindest teilweise entschlüsselt vorliegen.
Bei Cloud Computing werden Daten außerhalb des eigenen Unternehmens bei Cloud-Anbietern zusammen mit vielen anderen Daten gespeichert und verarbeitet. Infolge dessen sind besonders viele Daten bei einem Anbieter konzentriert, woraus sich ganz neue Probleme eines möglichen Datenmissbrauchs durch Insiderangriffe ergeben, bspw. von Administratoren. Darüberhinaus verschärft sich die Herausforderung an die Gewährleistung der Sicherheitsrichtlinien dadurch, dass durch die Komposition mehrerer Dienste von Drittanbietern komplexe neue Dienste bereitgestellt werden können. MimoSecco will hier Sicherheit gewährleisten, indem z.B. eine entfernte Verbindung eines mobilen Endgerätes mit einem Unternehmensserver genauso wie die Kommunikationsverbindung eines Dienstes mit einem anderen innerhalb einer physischen Ausführungsumgebung verschlüsselt wird. Neben der Datenverbindung sollen in MimoSecco neue Konzepte der Datenspeicherung entwickelt und überprüft werden, welche die Vertraulichkeitsanforderungen des Datenbesitzers sicherstellen sollen.

Fragmentiertes, örtlich verteiltes Sicherheitsmanagement

MimoSecco erlaubt es, Daten geschützt in der Cloud abzulegen und dennoch ein effizientes Arbeiten auf diesen Daten zu ermöglichen. Dies wird erreicht, indem die Daten geschickt auf mehrere unabhängige Cloud-Anbieter aufgeteilt werden. Auf dem Datenserver liegen die Daten in verschlüsselter Form, der Betreiber des Servers hat somit keine Kenntnis über den Inhalt der Daten. Eine über der Datenbank vorgenommene Indizierung wird teilverschlüsselt auf zwei weitere Server verteilt. Die Indizierung und das Verschlüsseln der Daten übernimmt der vertrauenswürdige Datenbankadapter. Anfragen an die Datenbank stellt der Cloud-Anwender über den Datenbankadapter. Dieser ermittelt durch Anfragen an die Indexserver die betroffenen Datensätze der verschlüsselten Datenbank. Diese werden dann durch den Datenbankadapter vom Datenserver abgerufen, entschlüsselt und dem Cloud-Anwender zur Verfügung gestellt. Bei Änderungen durch den Cloud-Anwender werden die bestehenden verschlüsselten Datensätze vom Datenbankadapter durch neue ersetzt und gegebenenfalls die betroffenen Indizes aktualisiert.

Token-basierte Verschlüsselungsmethoden

Ein zentrales Element ist die Nutzung zertifizierter Hardware-Sicherheitstoken. Dies sind spezielle, gegen physische Angriffe gesicherte Smartcards, die in unterschiedlichen Bauformen zur Verfügung stehen. Ein Sicherheitstoken muss an den Datenbankadapter angeschlossen sein. Der benötigte Schlüssel zur Entschlüsselung der Daten liegt nur im Sicherheitstoken vor. Liegen gültige Zertifikate des Cloud-Anwenders und gleichzeitig der vertrauenswürdigen SaaS-Anwendung vor, welche ebenso über eigene Sicherheitstoken abgesichert sind, gibt das Sicherheitstoken des Datenbankadapters den Schlüssel temporär frei, so dass die benötigten Daten entschlüsselt werden können. Nach erfolgter Bearbeitung der Daten wird der Schlüssel im Datenbankadapter wieder gelöscht.
Der Zugriff auf die Sicherheitstoken erfolgt über eine neu entwickelte Middleware. Diese wird als Baukasten gestaltet, so dass auf den jeweiligen Systemen (Endgerät, Saas-Anwendung, Datenbankadapter usw.) aus diesem Baukasten die dort jeweils benötigten Komponenten ausgewählt und eingesetzt werden können.

Ausgangssituation

- Mitarbeiter wollen mobil aber auch sicher auf Unternehmensdaten zugreifen
- Datenverarbeitung in der Cloud gilt als unsicher da Unbefugte Daten Zugriff auf die Daten erlangen können
- Öffentlicher Cloud-Anbieter hat theoretisch Zugang zu allen Daten

Zielsetzung

- MimoSecco sorgt für mehr Sicherheit bei der Verarbeitung von Daten in der Cloud und ermöglicht mobiles Arbeiten im Unternehmenskontext
- Mehrstufiges Sicherheitszonenkonzept erschwert Insiderangriffe bei Cloud-Anbietern
- Einsatz von Sicherheitstoken und Verschlüsselung ermöglicht bessere Kontrolle über den Zugriff auf die Daten der Nutzer

Koordinator	CAS Software AG, Spiros Alexakis
E-Mail	spiros.alexakis@cas.de
Telefon	+49 721 9638-215
Laufzeit	01.09.2010 – 31.08.2013
Partner	Karlsruher Institut für Technologie (KIT) WIBU-Systems AG www.mimosecco.de