



Presseinformation

Sealed Cloud

Technisch sicheres Cloud Computing

Die eigenen Datenbestände sind für Unternehmen wie ein gut gehüteter Schatz, egal ob es sich um Geschäftsgeheimnisse oder andere interne Dokumente handelt. Diese Daten in die Cloud auszulagern erscheint vielen Unternehmen immer noch riskant. Denn die sensiblen Informationen liegen dabei nicht mehr auf Festplatten im eigenen Haus, sondern bei einem Drittanbieter, der theoretisch darauf Zugriff nehmen könnte. Das Projekt Sealed Cloud entwickelt eine Lösung, um Daten in der Cloud besonders zu schützen und damit das Vertrauen von Unternehmen in Cloud-Dienste zu stärken.

„Versiegelung“ der Datenverarbeitung schafft Sicherheit

Dazu schafft Sealed Cloud eine „versiegelte“ Cloud-Computing-Infrastruktur. Sie soll mit technischen Mitteln hinterlegte Daten nachhaltig schützen. Ein ganzes System von Sicherheitsvorkehrungen schließt dabei über die gesamte Verarbeitung der Daten den Zugriff Unbefugter aus. Oftmals haben der Betreiber des Cloud-Dienstes und seine Mitarbeiter praktisch uneingeschränkten Zugriff auf die technische Infrastruktur und damit auf alle dort gespeicherten und verarbeiteten Informationen. Mit Sealed Cloud werden diese so genannten Insiderangriffe explizit ausgeschlossen. Damit bietet Sealed Cloud einen Schutz sowohl gegen externe als auch gegen interne Versuche Unbefugter, die sensiblen Daten abzurufen.

Bei der Sealed Cloud wird der Zugriff auf Daten, auch gegenüber dem Cloud-Anbieter, technisch derart erschwert oder sogar unmöglich gemacht, dass ein Lesen von Daten durch den Diensteanbieter oder den Cloud-Betreiber praktisch nicht mehr möglich ist. Angefangen bei den physischen Systemen über die genutzten Betriebssysteme und Middleware bis hin zu den Anwendungen wird ein abgeschlossenes Silo geschaffen, auf das der Zugriff von Unbefugten nicht möglich ist. In diesem Silo können die Daten sicher unverschlüsselt gehalten werden, was für die Verarbeitung der Daten notwendig ist. Der Zugriff wird über die gesamte Verarbeitung der Daten sowohl auf physischer als auch auf digitaler Ebene ausgeschlossen.

Offene und standardisierte Schnittstellenschicht für Cloud-Dienste

Sealed Cloud soll durch eine offene und standardisierte Schnittstellenschicht unternehmenskritischen Cloud-Diensten ein hohes Sicherheitsniveau und möglicherweise auch rechtliche Einfachheit bieten. Die Technologie wird am Beispiel zweier Lösungen im Bereich Software as a Service (SaaS) demonstriert. Mit deleGate soll zum einen ein Dienst angeboten werden, mit dem der Verfügungsberechtigte eines Unternehmens Zugangsberechtigungen zu

Cloud-Diensten verwalten und kontrolliert delegieren kann. Als zweites soll der etablierte Web-Privacy-Dienst ID|GARD, der für Unternehmen Vertraulichkeit für geschäftsrelevante Informationen im Internet bietet, auf die offene Schnittschicht portiert werden. Der Dienst soll die Privatsphäre von Anwendern im Internet schützen und so den Datenschutz sicherstellen.

Ausgangssituation

- Schutz von Anwenderdaten gegenüber Cloud-Anbietern nicht sichergestellt
- Kein einheitlicher technischer Datenschutzstandard für Public-Cloud-Lösungen
- Unklare Sicherheitslage mindert Vertrauen in Cloud-Dienste

Zielsetzung

- Versiegelte Cloud-Infrastruktur verhindert unbefugten Zugriff des Cloud-Anbieters auf Daten des Cloud-Anwenders
- Public-Cloud-Lösungen können so vertrauenswürdig sein wie Private-Cloud-Dienste
- Verbesserte technische und ggf. rechtliche Sicherheit erhöht Vertrauen in Cloud-Dienste

Koordinator	Unicon universal identity control GmbH, Dr. Hubert Jaeger
E-Mail	hubert.jaeger@unicon.de
Telefon	+49 89 4161 5988-100
Laufzeit	01.10.2011 – 30.09.2014
Partner	Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) SecureNet GmbH www.sealedcloud.de