SEALED CLOUD

EIN VERTRAUENSWÜRDIGES DATA CENTER OHNE ZUGRIFFSMÖGLICHKEITEN DES BETREIBERPERSONALS ZU KUNDENDATEN

WHITE PAPER

Uniscon GmbH -
The Web Privacy Company

Agnes-Pockels-Bogen 1
80992 München

Inhalt

Kurzfassung

Cloud Computing schafft viele neue Möglichkeiten und wirft dabei jedoch – insbesondere bei potenziellen Anwendern in Unternehmen – Fragen zur Sicherheit der häufig geschäfts- relevanten Daten auf:

a) Können Angreifer auf meine Daten zugreifen?
b) Sind meine Daten von jenen anderer Anwender sicher isoliert?
c) Können Administratoren des Betreibers auf meine Daten zugreifen?

Das White Paper stellt das Konzept der Sealed Cloud vor. Ein Sealed Cloud Data Center realisiert ein klares Prinzip: „Nur der Eigentümer der Daten hat Zugriff zu seinen Daten.“ Mit anderen Worten: Der Betreiber des Datenzentrums und seine Mitarbeiter werden mit technischen Mitteln vom Zugriff ausgeschlossen.

1. Cloud Computing – ein Datensicherheitsproblem?

Cloud Computing, d.h. Applikationen als Dienstleistungen aus dem Web, verspricht einen Umbruch in der Art und Weise der Nutzung von Informationstechnik – „IT aus der Steckdose“. Die Bereitstellung von Anwendungen im Web bringt neben vielen bekannten Vorteilen jedoch auch neue Risiken. Die von den Anwendungen verarbeiteten Nutzerdaten werden in einem Datenzentrum im Netz (in der Cloud) gespeichert und befinden sich somit auf Systemen, die vom Anwender nur schwer kontrolliert werden können.
Folgende Fragen zeigen die wesentlichen Sicherheitsbedenken, die geschäftliche Anwender heute vorrangig von der Nutzung von Cloud-Diensten abhalten:

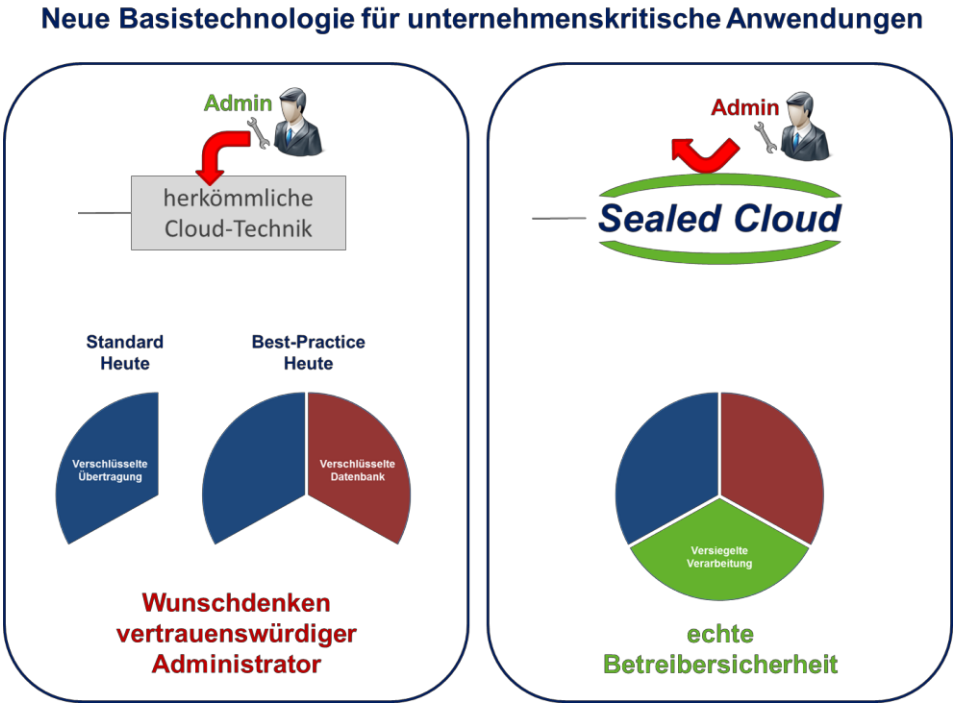
a) Können Angreifer auf meine Daten zugreifen?

b) Sind meine Daten von jenen anderer Anwender sicher isoliert?

c) Können Administratoren des Betreibers auf meine Daten zugreifen?

Das Sicherheitsniveau von Cloud-Infrastrukturen kann relativ hoch gegen Angriffe von außen gestaltet werden. Die Provider investieren signifikant in die Sicherheit gegen externe Angreifer als wesentliche Basis für Vertrauen des Kunden in die Dienstleistungen.

Jedoch können die Fragen (b) und (c) derzeit nicht zufriedenstellend beantwortet werden. Bislang setzen Cloud-Lösungen eine vertrauenswürdige Software und einen vertrauenswürdigen Betreiber der Cloud-Infrastruktur voraus. Neben verschiedenen technischen Maßnahmen hängt das Sicherheitsniveau jedoch sehr stark von der Qualität der internen Prozesse des Providers ab.



Viele öffentlich bekannt gewordene Datenverluste ohne externe Angriffe, selbst aus Bereichen mit höchsten Sicherheitsstandards (steuerrelevanten Kundendaten von Schweizer Banken, U.S.-

Regierungs- und Geheimdienstdokumente, Daten von Millionen von Kreditkartenkunden in den USA) sowie die außerordentlich hohe Dunkelziffer nicht veröffentlichter Vorfälle zeigen klar die Existenz vieler interner Schwachstellen heutiger Datenzentren allgemein. Denn überall wo Mitarbeiter Zugriff auf Daten haben, kann die Sicherheit ganz offensichtlich nicht garantiert werden.

Hier setzt das Konzept der „Sealed Cloud“ an, ein bereits in der EU und in den USA patentiertes Konzept der Firma Uniscon, das inzwischen im Rahmen der „Trusted Cloud“-Initiative des Bundeswirtschafts-ministeriums gefördert wird.

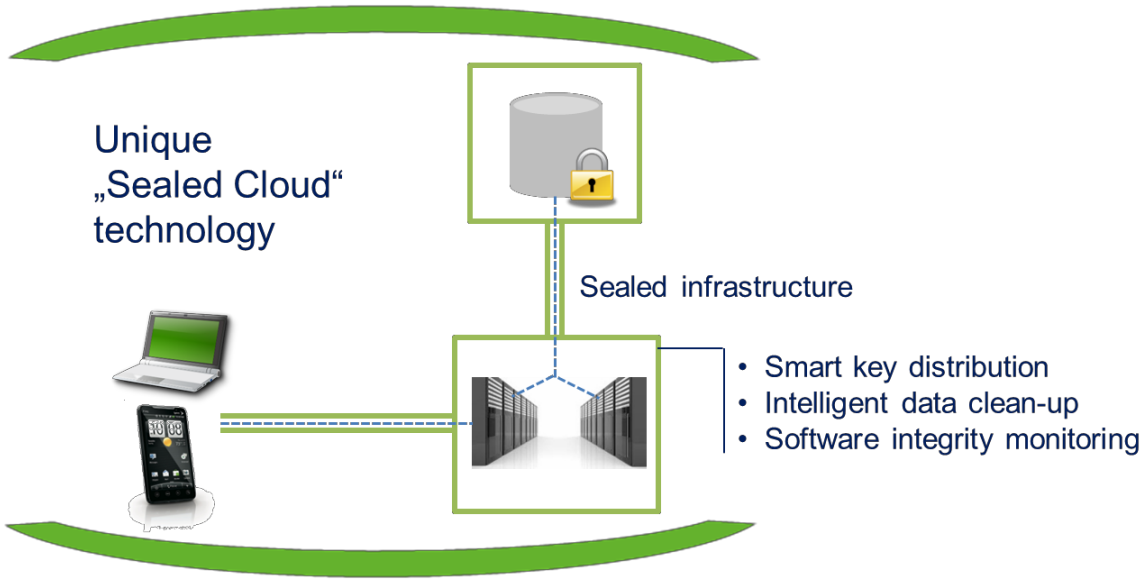
Ein Sealed Cloud Data Center realisiert ein klares Prinzip: „Nur der Eigentümer der Daten hat Zugriff zu seinen Daten.“ Mit anderen Worten: Der Betreiber des Datenzentrums und seine Mitarbeiter werden mit technischen Mitteln vom Zugriff ausgeschlossen.

2. Wie funktioniert eine Sealed Cloud?

Daten von Cloud-Applikationen sind in verschiedenen Bereichen möglichen Angriffen ausgesetzt:

1. Beim Transport zum und vom Datenzentrum,
2. im Storage-System / in der Datenbank und
3. während der Verarbeitung

Der Schutz beim Transport wird per Verschlüsselung, z.B. SSL mit 2.048 Bit Schlüssellänge realisiert. Das ist heute Standard und allgemein üblich.



Daten in der Datenbank bzw. im Storage-System werden ebenfalls verschlüsselt. Das ist zwar nicht unbedingt Standard, wird jedoch als Best Practice betrachtet und von Cloud- Systemen mit hohem Anspruch realisiert. Gängige technische Lösungen verschlüsseln die Daten in der Datenbank

bzw. im Storage-System auf Block-Ebene mit einem oder einer geringen Zahl systemweit gültiger Schlüssel. Der bzw. die Schlüssel werden dann in Schlüsselspeichern aufbewahrt.

Die Sealed Cloud geht hier in der heute bereits produktiven Realisierung für den Web Privacy Service iDGARD wesentlich weiter. Hier wird ein nutzerindividueller Schlüssel aus den Login-Informationen (Username, Passwort und ggf. weitere Daten) während des Anmeldevorgangs mit einem speziellen Algorithmus generiert. Mit diesem Schlüssel werden die Anwendungsdaten gefunden, entschlüsselt und in den Hauptspeicher geladen. Nach dem Abmelden werden die Daten wieder verschlüsselt und gespeichert. Der nutzerindividuelle Schlüssel wird anschließend zerstört. In der Datenbank für *n* Nutzer existieren somit *n* verschiedene Nutzerdatensätze, die jeweils individuell nach AES256 verschlüsselt sind. Da die Schlüssel nicht im System existieren, ist die Zugangshürde für interne und externe Angreifer außerordentlich hoch. Ein Angreifer müsste den AES256 knacken und dies jeweils separat für jeden Nutzerdatensatz.

Damit verbleibt der Hauptspeicher der Server als potentiell vulnerables Ziel für Insider- Angriffe, denn die Daten sind während einer aktiven Session dort in Klarschrift vorhanden. Ein Administrator könnte beispielsweise einen sogenannten Memory Dump ziehen und diesen zum passenden Zeitpunkt in aller Ruhe auswerten. Im Sealed Cloud-System werden die Server deshalb durch eine ganze Reihe zusätzlicher Maßnahmen geschützt. Einige Beispiele sind:

- Alle Applikationsserver befinden sich in elektromechanisch versiegelten Rack- Systemen.
- Die Server beinhalten nur flüchtige Speicher, d.h. nach Stromabschaltung befinden sie sich im „Lieferzustand“.
- Das verwendete Betriebssystem ist zusätzlich gehärtet und sperrt alle externen Zugänge.
- Das System meldet zwar Statusinformationen nach außen, es akzeptiert jedoch keine administrativen Anweisungen aus der Ferne. Für jegliche Administration muss das jeweilige Segment eines Serverschranks geöffnet werden.

Für die Durchführung eines administrativen Vorgangs wird über ein sogenanntes Trust Center von der dazu autorisierten Stelle eine Work Order erstellt. Diese wird dem betreffenden IT-Mitarbeiter auf sein Bluetooth Device, zusammen mit einem gültigen Zugangstoken, übermittelt. Über die Bluetooth-Schnittstelle des Systems kann der Zugang zu einem Schranksegment angefordert werden. Der Sealed Cloud Controller schließt daraufhin die in diesem Segment laufenden aktiven Sessions, deaktiviert die Server und stellt sie stromlos. Nach einer Wartezeit von etwa 15 Sekunden öffnet der Controller die Schrankverriegelung, nachdem sichergestellt ist, dass die Server keinerlei Daten mehr enthalten.

Nach dem Wartungsvorgang wird das Segment wieder verriegelt und die Server aktiviert. Beim Hochlauf wird der startende Softwarestack verifiziert, d.h. das System sucht nach eventuellen Abweichungen von der freigegeben, zertifizierten Software sowohl im Betriebssystem als auch im Anwendungsteil. Erkannte Abweichungen führen zum sofortigen Abschalten des Segments, da eine Manipulation nicht ausgeschlossen werden kann. Nach einem erfolgreichen Hochlauf wird das System im Betrieb kontinuierlich bezüglich Abweichungen vom definierten Normalverhalten überwacht. Auch hier führen Abweichungen zu Alarmen und zum Abschalten der betroffenen Segmente.

Die Kombination der beschriebenen Maßnahmen stellt sicher, dass im Datenzentrum kein Zugriff auf unverschlüsselte Daten erfolgen kann.

3. iDGARD – erste Anwendung der Sealed Cloud

Prinzipiell sind die Eigenschaften der Sealed Cloud für alle Arten von geschäftlichen Applikationen von Bedeutung, wenn diese Applikationen sensible oder gar vertrauliche Daten verarbeiten. Üblicherweise gelten Data Centers bei Sicherheitsexperten als generell nicht vertrauenswürdig. Sie empfehlen deshalb grundsätzlich lokale Ver- und Entschlüsselung auf dem Client-System.

Die Sealed-Cloud-Technologie schafft jedoch mittels Versiegelung ein vertrauenswürdiges Datenzentrum und ermöglicht dadurch dort die Realisierung von sicheren Anwendungen. Damit werden Anwendungen mit hohen Sicherheitsanforderungen einfacher und nutzerfreundlicher, da das normalerweise notwendige übergreifende und durchaus komplexe Schlüsselmanagement über viele Clients in vielen Bereichen entfallen kann.

So realisiert der Web Privacy Dienst iDGARD (www.idgard.de) sehr nutzerfreundlich sicherheitskritische Funktionen wie:

- Versiegelte Team Work Spaces für firmenübergreifende Projektarbeiten.
- Abhörsichere Nachrichten und Chats je Box austauschen.
- Automatisches Schlüsselmanagement in der Cloud - nur der Nutzer bestimmt, wer Zugriff auf seine Daten haben darf.
- Datenräume mit Funktionen für PDFs zum Schutz vor unerwünschter Weiterverbreitung.

iDGARD ist die Lösung für einen sichere und vertrauensvolle Kommunikation für alle Unternehmen.

4. Zusammenfassung

Unternehmen haben erkannt, das neben Schutz gegen externe Angriffe insbesondere auch ein Schutz gegen Insider erforderlich ist, denn die Mehrzahl der Datenverluste erfolgt über diesen Weg. Dies wird bei Überlegungen zu Cloud-Diensten deutlich, es betrifft interne Data Center jedoch ebenso. Die Sealed-Cloud-Technologie bietet hier einen pragmatischen und effektiven Ansatz.

Referenzen:

[1] www.idgard.de
[2] Web Privacy für Unternehmen, White Paper, Uniscon GmbH, 2012
[3] iDGARD Web Privacy, White Paper, Uniscon GmbH, 2012

Das Unternehmen

Die Uniscon GmbH wurde 2009 mit dem Ziel gegründet, technische Lösungen zu entwickeln, die es Usern erlaubt, sich im Internet sicher und frei zu bewegen. Mit unseren Produkten legen wir einen technischen Grundstein: Die Erfindung der Sealed Cloud – der Basistechnologie von iDGARD – gestattet Nutzern einen vertrauensvollen Umgang mit dem Internet. Mit unseren Produkten lösen wir das Problem des Datenschutzes – die bis heute größte verbliebene Herausforderung im Bereich Online-Sicherheit.

Kontakt

Claudia Seidl, Head of Corporate Communications
Uniscon GmbH
E-Mail: presse@uniscon.de
Telefon: +49 89 / 4161 5988 100

Version 1.2, September 2015