Compliance durch versiegelte Cloud

Hubert Jäger, Uniscon GmbH

Dr. Hubert Jäger war in leitenden Funktionen der Produktentwicklung, des Innovations- und Produktmanagements und Vertriebs bei großen High-Tech-Unternehmen tätig. Er ist Mitgründer und Geschäftsführer der Uniscon GmbH.

Das Hauptproblem beim Cloud-Computing sehen Unternehmen im Kontrollverlust über die Daten. Sie erfahren nämlich nicht, wer beim Cloud-Betreiber die verarbeiteten oder gespeicherten Daten mitliest oder kopiert. Anders ist das bei Anbietern, die ihre Anwendungen auf der Basistechnologie Sealed Cloud aufbauen [1]. Mit ihr werden Daten maschinell verschlüsselt und ein Zugriff auf sie durch eine Reihe technischer Maßnahmen verwehrt. Selbst dem Betreiber der Cloud bleibt der Zugang nicht nur beim Transfer und auf die Datenbank, sondern auch während der Verarbeitung der Daten verschlossen.

Wenn eigene Daten auf fremde Server fließen, verlieren Unternehmen die Kontrolle über diese. Laut einer im März 2013 veröffentlichten Studie der „Nationalen Initiative für Informations- und Internet-Sicherheit“ ist das für 65 Prozent der befragten Unternehmen der wichtigste Nachteil beim Cloud-Computing [2]. So verfügen zwar die meisten Cloud-Verträge über Datenschutzregelungen, gesetzliche Normen anderer Länder aber, wie der Foreign Intelligence Surveillance Act (FISA) oder der Patriot Act für die USA, höhlen diese Regelungen aus. Sie ermöglichen es z.B. US-Behörden Daten vom US-Cloud-Betreiber zu verlangen, ohne das betroffene Unternehmen informieren zu müssen.

Außerdem können die Betreiber die ihnen anvertrauten Daten jederzeit mitlesen, da diese bei der Verarbeitung immer in Klarschrift vorliegen. Daher sind sensible Dokumente, die per E-Mail verschickt oder in Public Share Rooms abgespeichert werden, keineswegs sicher. Unternehmen müssten für ihre Geschäftskommunikation eigentlich stets in eigener Regie eine Private Cloud nutzen, in der zum Beispiel E-Mails extra verschlüsselt oder besonders gesicherte Schutzräume vorgesehen sind. Im täglichen Ablauf aber erfolgt die digitale Kommunikation öfter ungeschützt als man denkt: Möglicherweise betreibt ein Unternehmen sogar eine Private Cloud, in der Unternehmensdaten sicher verwahrt sind und bleiben. Allerdings können die Mitarbeiter trotzdem noch auf die Daten zugreifen. Auch bei firmenübergreifenden Projekten können viele Firmen meist in der digitalen Kommunikation mit Partnerunternehmen diesen Schutz nicht aufrecht erhalten. Das Schlüsselmanagement erscheint Mitarbeitern zu kompliziert; E-Mails mit sensiblen Dokumenten im Anhang werden dann lieber unverschlüsselt ausgetauscht.

Ein weiterer Kontrollverlust entsteht durch den vermehrt auftretenden Gebrauch von Applikationen (Apps) in mobilen Endgeräten. Diese synchronisieren automatisch Daten in die jeweilige Cloud des Anbieters – in oft fremde Länder mit laxeren Datenschutzbestimmungen als in Deutschland. Was dazu führt, dass Verantwortliche nur dann wissen können, wer tatsächlich Zugang zu vertraulichen Unternehmensdaten hat, wenn diese von Mitarbeiter weder über Smartphone bzw. iPhone aufgerufen, verschickt oder abgespeichert werden.

Kontakt

Uniscon GmbH
Geschäftsführung
Agnes-Pockels-Bogen 1
80992 München
Tel.: + 49 89 / 41615988-100
E-Mail: hubert.jaeger@uniscon.de
URL: http://www.uniscon.de

Bild 1: Eine Cloud muss nicht nur ökonomisch und flexibel, sondern auch sicher sein.

Bild 2: Das Konzept Sealed Cloud umfasst den Schutz vor logischen und physischen Zugriffen.

Über IT-Sicherheit verfügt heute nur noch, wer die Daten einerseits gegen Angriffe von außen schützt, andererseits das firmenübergreifende Weiterleiten sowie den internen Verlust und Missbrauch verhindert. Was IT-Sicherheitsexperten als derzeit unmöglich bezeichnen [3] . Aus diesem Grund fördert das Bundesministerium für Wirtschaft und Technologie im Rahmen der Initiative „Trusted Cloud“ die Weiterentwicklung der Sealed Cloud, die von einem Konsortium aus dem Münchner Unternehmen Uniscon GmbH, der Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) und der SecureNet GmbH vorangetrieben wird. Diese Basistechnologie verhindert, dass unbefugte Dritte Daten einsehen – seien es nun Angreifer von außen oder der Betreiber einer Cloud selbst. Sie wahrt die Vorteile des Betreibermodells einer Public Cloud, erhöht aber gleichzeitig das Vertrauen in die Sicherheit.

Denn sie schafft mittels „Versiegelung“ ein vertrauenswürdiges Datenzentrum, in dem sich sichere Anwendungen aufbauen lassen.

Anwendungen auf der Sealed-Cloud-Plattform

Mit der Sealed-Cloud-Technologie erreicht ein Rechenzentrum ein zuvor nicht bekanntes, hohes Sicherheitsniveau. So entwickelt zum Beispiel das auf die Web Application Security spezialisierte Unternehmen SecureNet eine Anwendung zum Management von Identitäten für webbasierte Dienste. Damit sollen Unternehmen die Kontrolle über solche – vielfach unternehmenskritische – Dienste, die durch Mitarbeiter und Partner genutzt werden, zurück erhalten. Auch das Münchner Unternehmen Uniscon GmbH bietet einen Dienst an, der Unternehmen einen maschinell verschlüsselten Austausch von Dokumenten mit Kunden, Partnern und Lieferanten über das Internet ermöglicht. Wobei folgende Fragestellungen beantwortet werden: Wie tauscht man firmenübergreifend vertrauliche Dokumente aus? Wie arbeiten mehrere Mitarbeiter unterschiedlicher Unternehmen an einem vertraulichen Dokument? Wie stellt man sicher, dass die Unterlagen auf deutschen Servern verbleiben?

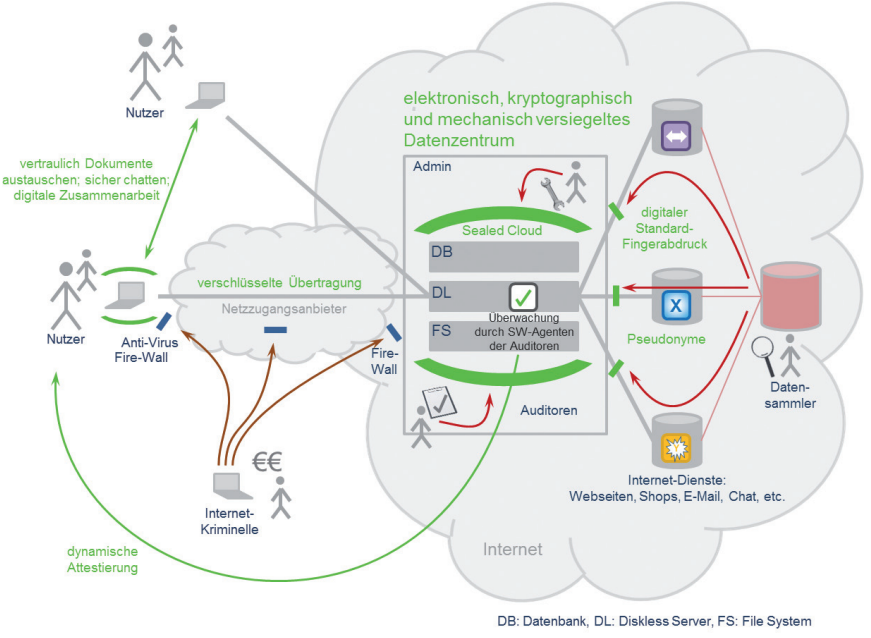
So funktioniert die Sealed Cloud

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

1. Beim Transport zum und vom Datenzentrum
2. Im Storage-System in der Datenbank
3. Während der Verarbeitung

Per Verschlüsselung, z.B. SSL mit 2048 Bit Schlüssellänge lassen sich die Daten beim Transport schützen. Das ist Standard und auch allgemein üblich. Daten in der Datenbank bzw. im Storage-System werden ebenfalls verschlüsselt. So arbeiten heute Cloud-Systeme mit hohem Anspruch. 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. Den oder die Schlüssel bewahren die Betreiber dann in Schlüsselspeichern auf.

Bild 3: Das Sealed-Cloud-System.



Die Sealed Cloud geht wesentlich weiter: Hier generiert das System während des Anmeldevorgangs einen nutzerindividuellen Schlüssel aus den Login-Informationen wie Benutzernamen, Passwort und eventuell weiterer Daten. Er dient dazu, die Anwendungsdaten zu finden, zu entschlüsseln und in den Hauptspeicher zu laden. Nachdem sich der Anwender am Ende jeder Session abgemeldet hat, werden die Daten wieder verschlüsselt und gespeichert. Danach zerstört das System den individuellen Schlüssel. In der Datenbank existiert für jeden Nutzer ein eigener Datensatz, der jeweils individuell nach AES256 verschlüsselt ist. Da die Schlüssel im System nicht existieren, ist die Zugangshürde für interne und externe Angreifer außerordentlich hoch. Ein Angreifer müsste den AES256 knacken und dies separat für jeden einzelnen Nutzerdatensatz.

Damit bleibt der Hauptspeicher aller Server als potenziell vulnerables Ziel für Insider-Angriffe: 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 sind 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.
- Bevor ein Mitarbeiter oder Angreifer an die Server gelangt, werden alle unverschlüsselten Daten gelöscht.
- Das verwendete Betriebssystem ist zusätzlich gehärtet und sperrt alle externen Zugänge.
- Das System meldet zwar Statusinformationen nach außen, akzeptiert jedoch keine Befehle von außerhalb.

Um einen administrativen Vorgang ausführen zu können, muss über ein „Trust Center“ von der dazu autorisierten Stelle ein Arbeitsauftrag erstellt werden. Erst wenn der betreffende IT-Mitarbeiter diesen zusammen mit einem gültigen Zugangstoken auf sein Bluetooth Device übermittelt bekommen hat, kann er über die Bluetooth-Schnittstelle des Systems Zugang zu einem Schranksegment anfordern. 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 auf diese Weise sichergestellt ist, dass die Server keinerlei Daten mehr enthalten.

Bild 4: Compliance im Unternehmen.

Nach dem Wartungsvorgang wird das Segment wieder verriegelt und die Server werden aktiviert. Beim Hochlauf wird der startende Software Stack verifiziert, d.h. sowohl im Betriebssystem als auch im Anwendungsteil wird nach eventuellen Abweichungen von der freigegeben, zertifizierten Software gesucht. Bei Abweichungen schaltet sich das Segment sofort ab, um mögliche Manipulationen auszuschließen. Nach einem erfolgreichen Hochlauf wird das System auch im Betrieb kontinuierlich bezüglich Abweichungen vom definierten Normalverhalten überwacht und ggf. das betroffene Segment abgeschaltet.

Durch diese Kombination der beschriebenen Maßnahmen ist bei der Sealed Cloud sichergestellt, dass im Datenzentrum kein Zugriff auf unverschlüsselte Daten erfolgen kann.

Zertifizierung der Prozesse und Abläufe

Durch eine Reihe von technischen Maßnahmen und einer vertrauenswürdigen Kontrollinstanz soll die maschinelle Versiegelung der Sealed Cloud gewährleistet sein und bleiben. Dabei werden die Server um grundlegende Sicherheitsfunktionen erweitert: Auf Basis der in den Servern eingesetzten Hardware-Komponenten wird ein Codewort generiert, das bei einer Manipulation der Server diese anzeigt. Zum Beispiel könnte dadurch festgestellt werden, wenn bei Servern, die ursprünglich keine persistenten Speichermedien enthalten, solche integriert würden. Gemeinsam mit einem speziell angepassten Betriebssystem und der eingesetzten, zertifizierten und freigegebenen Software entsteht dadurch eine vertrauenswürdige Plattform. Erst nachdem das zertifizierte System in einem definierten Release-Prozess überprüft hat, ob die Software- und Hardware-Komponenten zusammenpassen, setzt es sich in Betrieb.

Zurzeit wird daneben auch zusammen mit einer neutralen Zertifizierungsstelle an einer „dynamischen Attestierung“ gearbeitet. Dabei soll bei laufendem Betrieb geprüft werden, ob auch weiterhin alle Voraussetzungen für den zertifizierten Ablauf erfüllt sind. Treten Abweichungen auf, werden sofort geeignete Maßnahmen ergriffen: Zum einen werden die betroffenen Server oder Serverteile außer Betrieb genommen, zum anderen ergeht eine Meldung an die auditierende Stelle. Damit gibt es eine technische Kontrolle, die Manipulationen bei Wartungen oder interne Angriffe ausschließen.

Einsatzbereiche für Unternehmen

In fünf Bereichen haben Unternehmen Haftungsrisiken, wenn sie vertraulichen Daten auf fremde Server parken:

1. *Einsatzmöglichkeit bei Geschäftskommunikation mit Externen*
   E-Mails sind wie zuvor erwähnt für vertrauliche Informationen und Dateien keine sichere Option, weil die E-Mail-Provider Einsicht in die Mails haben [4]. Außerdem können Inhalte und Anhänge während des Transfers abgefangen werden, z.B. von Analysefirmen, die Profile aus den Inhalten der E-Mails erstellen. Die Sealed Cloud Technologie ermöglicht einen gesicherten Mail-Verkehr.
2. *Daten bleiben auf deutschen Servern*
   Sealed Cloud schützt Dokumente vor unbefugten Mitlesern, auch von den US-Abfragen auf die Server der IT-Giganten Microsoft, Google, Facebook etc. Denn sie werden auf den heimischen, verschlossenen Servern verarbeitet und gespeichert und sind nur für Nutzer zugänglich.
3. *Dokumentenschutz auch bei mobilen Devices*
   Immer mehr Mitarbeiter verschicken sensible Informationen mit dem Smartphone oder iPhone. Auch laden sie wichtige Dokumente herunter, um sie sich anzusehen. Auf iPhone und Android können Unternehmen mit einer Sealed-Cloud-Anwendung dafür sorgen, dass vertrauliche Dokumente im Hintergrund nicht versehentlich in die iCloud bzw. Google Drive synchronisieren – und somit im Ausland gespeichert und von Unbefugten gelesen werden.
4. *Schlüsselmanagement mit der Sealed Cloud*
   Die IT-Administration von Unternehmen hat riesige Aufwände, um einen kontinuierlichen Datenabgleich mit den vielen verschiedenen Anbietern von Web-Accounts zu erreichen. Deshalb leben Accounts oft noch ungewollt weiter und laden zum Missbrauch ein. Mit der Sealed Cloud steht eine Technologie zur Verfügung, auf der man Anwendungen für eine zentrale Speicherung und Verwaltung von Web-Accounts implementieren kann.
5. *Verwischen der Datenspuren beim Surfen*
   Mitarbeiter hinterlassen mit ihren Internet-Suchanfragen und anderen Webaktivitäten Datenspuren, die oftmals detailliert Aufschluss über die laufenden Arbeiten und Projekte geben: Mit Big Data, einer neuen Technologie, mit der große, unstrukturierte Datenmengen in Echtzeit analysiert werden, können diese ausgewertet und zurückverfolgt werden. So lassen sich Pläne und Ziele möglicher M&A-Aktivitäten, geplante Produkte und Technologien und die Vorbereitung von Partnerschaften und Kooperationen ausforschen. Zwar steckt laut Michael Kleinemeier, Mitglied des Bitkom-Präsidiums, „in Deutschland Big-Data noch in den Kinderschuhen“, doch sieht er „ein enormes Wachstumspotenzial“ [5]. Um dieser Entwicklung entgegenzuwirken, kann der gesamte Web-Verkehr über die Sealed Cloud geleitet, die personen- und firmenbezogene Merkmale durch einheitliche ersetzt werden: So können Suchanfragen pseudonymisiert werden.

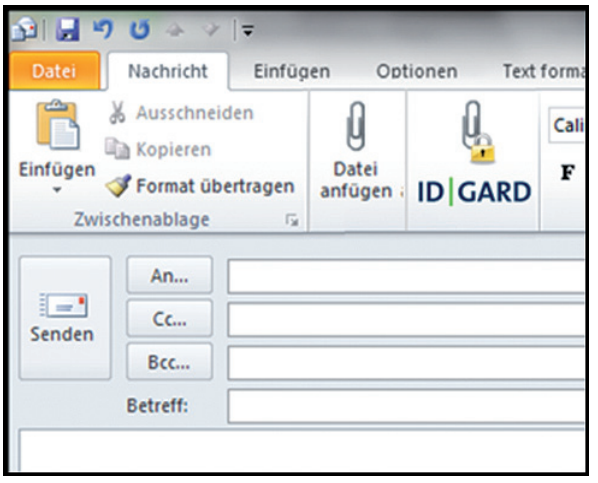


Bild 5: Ein Klick im IDGARD Add-On genügt.

Literatur

[1] Jäger H. et.al.: Sealed Cloud - A Novel Approach to Safeguard against Insider Attacks, angenommen für den Workshop „Wissenschaftliche Ergebnisse der Trusted Cloud Initiative” des Bundesministeriums für Wirtschaft und Technologie, Juli 2013.

[2] Karlstetter, F.: Negative Aspekte beim Auslagern von Daten in die digitale Wolke. URL: http://www.searchcloud-computing.de/sicherheit/risk-management/articles/398303/, Abrufdatum 18. 03.2013.

[3] Beuth, P.: Wir leben in einem Überwachungsstaat. URL: http://www.zeit.de/digital/datenschutz/2013-03/bruce-schneier-interview-security.

[4] Brandl, S.; Böhme K.: IT-Sicherheitslage m Mittelstand 2012. Initiative Deutschland sicher im Netz. URL: https://www.sicher-im-netz.de, Abrufdatum 11.03.2013.

[5] Daten sind der wichtigste Rohstoff der Welt. URL: http://www.bitkom.org/de/presse/8477_75285.aspx:, Abrufdatum 28.03.2013.

Schlüsselwörter:
Compliance, Sealed Cloud, Technischer Datenschutz, Auftragsdatenverarbeitung, Datensicherheit, Schutzniveau, Berufsgeheimnisse, Offenbarung vermeiden, Cloud-Computing, Cloud-Sicherheit, sichere Geschäftskommunikation

Compliance through a Sealed Cloud

For businesses, the main problem with cloud computing is the loss of control over own data. After all, one cannot know what cloud provider staff might read or copy processed or stored data. Not so with providers based on Sealed Cloud technology. This basic technology encrypts all data, and any access is rendered impossible by a series of technical measures. Not even the cloud provider has access to the data, not only during transfer and within the database, but also during data processing.

Keywords:
compliance, sealed cloud, cloud-computing, privacy, privacy by design, data protection, secure business communications, protection level, avoid data disclosure