Link: http://www.computerwoche.de/a/wie-cloud-daten-am-besten-zu-schuetzen-sind,3096885

Forrester zu Cloud Data Protection

Wie Cloud-Daten am besten zu schützen sind

Datum: 21.04.2015
Autor(en): Stanislav Wittmann

Die Unsicherheit von Dokumenten und Daten in der Cloud hält viele Anwender (zurecht) davon ab, Kritisches dort abzulegen. Werkzeuge und Lösungsansätze verschiedenster Anbieter versprechen Abhilfe. Sind das nur leere Versprechungen oder gibt es die sichere Wolke wirklich?

Cloud Data Protection (CDP) ist im unternehmerischen Umfeld nicht nur wichtig, sondern obligatorisch. Für ihre **Marktstudie "Cloud Data Protection Solutions"**[1] befragten die Analysten von Forrester Research 17 Anbieter nach ihren Security-Produkten und -Strategien für eine sichere und geschützte Wolke. Wichtige Erkenntnis: Die Security-Einstellungen der Cloud-Anbieter reichen oft nicht aus. Security Experten möchten aus der Auswahl von Sicherheitseinstellungen frei wählen - auch und gerade bei etablierten Cloud-Anbietern wie Dropbox, OneDrive, Gmail & Co. Denn im Falle eines Incidents wird nach der Verantwortung gefragt.

Security-Spezialisten wissen das und misstrauen den Sicherheitseinstellungen der etablierten Cloud-Anbieter - durchaus berechtigt. Spätestens die NSA-Affäre hat gezeigt, was heutzutage möglich und zudem gängige Praxis ist. Eine eigene Verschlüsselung der hochgeladenen Daten wäre so eine zusätzliche Sicherheitsmaßnahme, der sich Security Experten bedienen. Laut Forrester gaben **rund 35 Prozent der der befragten Security-Experten an, Daten vor dem hochladen zu Cloud-Anbietern zu verschlüsseln.**[2] Misstrauen gegenüber Cloud-Diensten könnten auch externe Auditoren von besagten Unternehmen haben. Denn diese haben nicht nur die Aufgabe, eine Zertifizierung zu bestätigen oder voranzutreiben. Auch Auditoren stehen in der Verantwortung. Gerade wenn es um sensible Daten von kritischer Infrastruktur aus dem Finanzsektor oder dem Gesundheitswesen geht.

Security-Appliances helfen

"Der Einsatz zertifizierter Security-Appliances, welche für den Einsatz in der Cloud optimiert sind, hilft Anwendern und Auditoren bei der Umsetzung von Cloud Projekten gleichermaßen", so Olaf Hansel, Geschäftsführer des Internetproviders **cx-solutions**[3] in Niedereschbach. "Für den Anwender erleichtern sie den Umgang mit Verschlüsselung und ermöglichen die Kontrolle des Datenflusses. Auditor und Unternehmen profitieren von bereits zertifizierten Lösungen."

Die Aufklärung von Security Incidents ist für die Experten ebenfalls wichtig. Bei der Verwendung von Cloud-Diensten wird das aber tendenziell schwieriger. Zur Tataufklärung werden die Protokolldateien benötigt. Forrester macht klar, dass Cloud-Anbieter diese ungern herausgeben, da der Datenverkehr zunehmend **mandantenfähig**[4] verläuft. Selbst wenn die Security-Abteilungen an die Daten herankommen, ist die Auswertung der Daten aufgrund der Menge und mangelnden Übersicht komplex. Für den Cloud-Anbieter hat diese Datenverwaltung durchaus Vorteile. Die zentrale und einmalig fällig Wartung und der geringere Speicher- und Kostenbedarf sind nur einige der Gründe, die für den Provider sprechen.

[Hinweis auf Bildergalerie: **Die besten Security-Appliances**] gal1

Zusätzlich macht die Forrester-Studie klar, dass für Security-Experten die Identität der Cloud-Benutzer im Vordergrund steht. Durch mobiles Arbeiten und Geschäftsreisen muss sichergestellt sein, dass ausschließlich autorisierte Benutzer auf Cloud-Dateien zugreifen können und Dateien sich nicht verfälschen lassen.

Fünf Lösungsvorschläge für CDP

Sobald man sich für das CDP-Modell entscheidet, stellt sich die Frage, wo und wie der Anbieter Dateien verschlüsselt, bevor sich diese lagern lassen. Forrester stellt hierfür fünf grundsätzliche Möglichkeiten dar:

- **CDP Encryption gateway in the cloud**

Die erste Möglichkeit stellt die Verschlüsselung in der Cloud selbst dar. Und zwar vom Cloud-Provider. Diese Möglichkeit sieht Vorteile im Benutzermanagement und setzt kein großes Hintergrundwissen voraus. Dagegen haben Nutzer dieser Lösung wenig Einsicht in die Verwaltung. Insgesamt erfordert diese Lösung gegenüber dem Anbieter einen gewissen Grad an zusätzlichem Vertrauen.

- **CDP encryption gateway on-premises**

Dagegen gibt es die Möglichkeit, Dateien selbstständig zu verschlüsseln, bevor diese hochgeladen werden. Für dieses Verfahren sprechen unter anderem die klare Benutzerverwaltung und die daraus resultierende Kontrolle über die Schlüssel respektive die Passwörter. Auf der anderen Seite steht ein erhöhter Ressourcenbedarf. Dafür werden Sie mit der Kontrolle der Schlüsselverwaltung belohnt.

- **CDP encryption using a user-side plug-in**

Vor dem Upload kann der Benutzer in dieser Lösung die Dateien selbst verschlüsseln. Dabei kann er ein dafür vorgesehenes Plug-in nutzen. Für diese Alternative spricht ein hoher Grad an Kontrolle über die Schlüssel. Folglich lassen sich so Incidents besser aufklären. Gegenüber stehen erneut höhere Kosten durch mehr Verwaltungsarbeit und eventuell nötige Lizenzen.

- **Centralized Drive Encryption in the cloud at a virtual or physical level**

Diese Methode ähnelt der ersten. Die Verschlüsselung erfolgt wiederum in der Cloud. Dabei lassen sich Dateien aus einer virtuellen Maschine verschlüsseln und anschließend physisch lagern.

Alternativ kann ein **Hypervisor**[5] die Dateien verschlüsseln und sichern. Bei Verwendung dieser Methode lässt sich beispielsweise der Datenstrom gut verfolgen, dafür ist die Abhängigkeit vom Cloud-Provider zwecks Sicherheit relativ hoch.

- **Cloud Data Governance Platforms**

Zum Abschluss stellt Forrester noch eine Möglichkeit vor, die ohne Verschlüsselung auskommt. Stattdessen lässt sich genau nachvollzeihen, wer auf welche Daten zugreift. Die Software wird hierfür in der Regel zur Verfügung gestellt. Der Nachteil dieser Lösung liegt auf der Hand: Es gibt keine Verschlüsselung.

Die Analysten vergleichen in einer Marktübersicht die verschiedenen Lösungen in den einzelnen Bereichen miteinander. Wer Details zu den Anbietern erfahren möchte, kann die Studie **hier**[6] erwerben.

Qualität durch Verschlüsselung

Ein Qualitätskriterium für die Cloud ist die Verschlüsselung. Hierzu macht Forrester deutlich, dass Security-Experten hohen Wert darauf legen, Dateien vor dem Upload zu verschlüsseln. Provider bevorzugen zudem die "**Zero-Knowledge-Policy**[7]", da diese so keinen Zugriff auf die Informationen haben. Denn sobald Cloud-Anbieter Daten entschlüsseln können, besteht konkrete Gefahr, dass Daten massenhafter Überwachung ausgesetzt sind. Olaf Hansel resümiert: "Verschlüsselung und gesicherte Datenübermittlung haben ihren Preis - sei es finanziell oder in Form von zusätzlich notwendigen Maßnahmen. Um ein vielfaches höher ist jedoch der Preis für den Verlust wichtiger Daten."

[Hinweis auf Bildergalerie: **Die wichtigsten Cloud-Zertifikate**] gal2

Und nun? Verschlüsseln oder nicht? Und wenn doch, dann gleich alle Daten, wie es zum **Beispiel Edward Snowden** [8]empfiehlt oder nur partiell? Dem Cloud-Anbieter vertrauen und verschlüsseln lassen oder doch das Prinzip "Bring your own encryption" (ByoE) nutzen? Letztlich ist es eine individuelle Entscheidung des Unternehmens, die in einer wirklich exakten **Risikobeurteilung**[9] zu treffen ist. Die Kosten-Nutzen-Relation darf auch nicht außen vor bleiben.

Die Kehrseite der Cloud-Verschlüsselung

Die Verschlüsselung von Cloud-Daten kann auch zu Problemen führen. So stellt sich zum Beispiel die Frage, wie nach verschlüsselten Dokumenten zu suchen ist. Security-Experten sollten bedenken, wie stark verschlüsselt wird. Denn es gilt, Inhalte beispielsweise vor **Reverse Engineering**[10] zu schützen. Hinzu kommt die gewünschte möglichst schnelle Verfügbarkeit von Daten - überall und zu jeder Zeit. Ein hoher Komfort für die Nutzer mit minimalen Latenzzeiten also - im Idealfall gepaart mit einer schnell funktionierenden Ver- und Entschlüsselung. Auch stellt Forrester fest, dass Datenlecks schwer aufzuklären sind und die **Data Loss Prevention (DLP)**[11] häufig unzureichend funktioniert. Dagegen hilft eine Optimierung des DLP-Systems selbst und der entsprechenden Richtlinien (Policy).

[Hinweis auf Bildergalerie: **Viivo - Cloud-Speicher verschlüsseln**] gal3

Zusammenfassung der Studie

Ein ganzheitliches Cloud-Konzept schafft Vertrauen. Dabei spielt neben der Verschlüsselung eine klare und benutzerfreundliche Zugänglichkeit eine wichtige Rolle. Denn laut Forrester geben die meisten befragten Security-Experten an, dass die Produktivität Hand in Hand mit den Sicherheitseinstellungen gehen soll. Darüber hinaus ist die Nachvollziehbarkeit des Datenverkehrs wichtig - kommt es zum Breach, muss feststellbar sein, wer welche Dokumente hoch- oder runtergeladen hat. Erfüllen CDP-Lösungen diese Anforderung nicht, sind Sie zum Scheitern verurteilt.

Mehr Kontrolle bedeutet aber auch mehr Aufwand. Sobald Sie einen höheren Grad an Sicherheit erreichen möchten, erhöhen sich sowohl administrativer Aufwand als auch die Kosten.

Fazit

Durch die Zunahme der Datenmenge steht eine strikte Abkehr vom Cloud Computing nicht zur Debatte. Für Unternehmensanwender gibt es keine realistische Alternative, was den Umgang mit großen Datenmengen angeht.

Bevor Daten in die Cloud gestellt werden, kann es sinnvoll sein, diese zu klassifizieren und nur ausgewählte Daten in eine Cloud hochzuladen. Für solche Entscheidungen kann eine **Business Impact Analyse**[12] helfen. In jedem Fall gilt es bei der Auswahl des Cloud-Anbieters, auf einen **starken und verlässlichen Datenschutz sowie eine akzeptable Benutzerfreundlichkeit**[13] zu achten. Die lokale Gesetzgebung des Providers sollte ebenfalls in die Entscheidung einfließen.

Die Marktentwicklung ist ebenfalls ein spannendes Thema. In dieser Branche spielt Vertrauen eine große Rolle und dieses könnte im **amerikanischen Markt dahinschwinden**[14]. Das wiederum könnte dem europäischen und asiatischen Markt einen Wettbewerbsvorteil verschaffen. (sh)

Links im Artikel:

[1] **https://www.forrester.com/Market%2BOverview%2BCloud%2BData%2BProtection%2BSolutions/fulltext/-/E-res120911**
[2] **https://spideroak.com/privacypost/business-the-cloud/the-importance-of-encryption-for-companies-in-the-cloud/**
[3] **http://www.cx-solutions.de/home.php**
[4] **http://www.enterprisecioforum.com/de/blogs/rickblaisdell/mandantenf%C3%A4higkeit-der-cloud-die-vorteil**
[5] **http://www.itwissen.info/definition/lexikon/virtual-machine-monitor-VMM.html**
[6] **https://www.forrester.com/Market%2BOverview%2BCloud%2BData%2BProtection%2BSolutions/fulltext/-/E-res120911**
[7] **http://www.theguardian.com/technology/2014/jul/17/edward-snowden-dropbox-privacy-spideroak**
[8] **http://de.ciphercloud.com/blog/edward-snowden-importance-cloud-data-encryption/**
[9] **http://www.beuth.de/de/norm/din-en-31010-vde-0050-1-2010-11/134170246**
[10] **http://www.businessdictionary.com/definition/reverse-engineering.html**
[11] **https://www.forrester.com/Rethinking%2BDLP%2BIntroducing%2BThe%2BForrester%2BDLP%2BMaturity%2BGrid/fulltext/-/E-RES61231?objectid=RES61231**
[12] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/3_BusinessImpactAnalysieren/BIA_node.html**
[13] **https://netzpolitik.org/wp-upload/Ueberwachtes-Netz-Markus-Beckedahl-Andre-Meister.pdf**
[14] **http://www.focus.de/finanzen/news/netzsplitter-nsa-affaere-vertrauen-in-die-cloud-sinkt_aid_1094165.html**
