Alle Partner in einer Wolke

Clouds für definierte Gruppen, sogenannte Community Clouds, schützen gespeicherte Inhalte durch definierte Eintrittsbarrieren

Datenschutz ist beim Cloud Computing nach wie vor ein kritischer Punkt – und wird es auch bleiben. RZ-Verantwortliche, die größere Datenmengen auslagern oder Möglichkeiten zum Austausch mit anderen Unternehmen schaffen wollen, sollten daher auf größtmögliche Sicherheit achten. Eine Lösung können Community Clouds sein.

In die bekannten Anwendermodelle von Public, Private und Hybrid Cloud eingeordnet, rangiert die Community Cloud zwischen dem privaten und dem öffentlichen Wolken-Modell. Hier schließen sich Unternehmen, Institutionen oder Behörden mit ähnlichen Interessen zu einer Community zusammen. Entweder betreibt eine der Partner-Institutionen die Cloud-Infrastruktur oder ein Dritter, beispielsweise ein Cloud Service Provider (CSP). Die gemeinsamen physischen Ressourcen stehen als Shared Infrastructure ausschließlich diesem eingeschränkten Nutzerkreis zur Verfügung. Besonders in Hinblick auf gemeinsame Teilprozesse oder Projekte unterschiedlicher Unternehmen bietet die Community Cloud enorme Vorteile für die Zusammenarbeit.

Dabei sind verschiedene Einsatzszenarien denkbar: Unternehmen mit Partnerstrukturen, die den Zugriff auf gemeinsame Ressourcen realisieren wollen, bietet sich die Community Cloud an. In der Automotive-Industrie hat sich dieses Modell beispielsweise etabliert: OEMs, Zulieferer und Partner nutzen eine gemeinsame Infrastruktur für den sicheren Austausch kritischer Entwicklungs-, Einkaufs-, und Produktionssteuerungsdaten. Ein unabhängiger Verein betreibt die technische Infrastruktur dieses Netzwerks.

Quelle: Zimory

Eine Community Cloud sollte verschiedene Anforderungen erfüllen, damit sie ihren Zweck erfüllt und möglichst sicher betrieben werden kann (Abb. 1).

Vertrauen durch Kontrolle und einheitliche Standards

Die Community Cloud bringt einige zentrale Vorteile: Sie stellt einen Schutzraum dar, in dem mehrere Teilnehmer untereinander sensible Daten – beispielsweise vertrauliche Entwicklungs-, Logistik- oder Steuerdaten – austauschen. Im Vergleich zur klassischen Public Cloud bietet die Community Cloud ein deutliches Mehr an Sicherheit: Das ist durch den beschränkten Nutzerkreis begründet, vor allem wenn dieser über klar definierte Eintrittsbarrieren wie Audits oder Zertifizierungen verfügt. Diese Barrieren sollten gleichzeitig das Einhalten von Mindeststandards sicherstellen, auf die sich die Teilnehmer der Community Cloud im Vorfeld geeinigt haben.

Das kann beispielsweise die ISO 27001 für Informationssicherheit sein, die Sicherheitsempfehlungen für Cloud-Computing-Anbieter des BSI (Bundesamt für Sicherheit in der Informationstechnik) oder der Einsatz von FIPS 140-2 (Federal Information Processing Standard) zertifizierten kryptografischen Modulen, die beispielsweise für die Zusammenarbeit mit US-amerikanischen und kanadischen Behörden Pflicht sind.

Die verschiedenen Parameter wie Security Policies, Data Segregation, Business Continuity, Intrusion Prevention oder Compliance-Anforderungen definiert die Nutzer-Gemeinschaft spezifisch nach ihren eigenen Ansprüchen und den erforderlichen rechtlichen Rahmenbedingungen. Je einheitlicher und höher die Standards sind, desto größer ist auch das Vertrauen in die Sicherheit der Community Cloud – besonders wenn die Standards durch unabhängige Dritte beispielsweise durch Zertifizierungen bestätigt sind.

Das Netz – der Weg in die Community

Der Zugang zur Public Cloud erfolgt in der Regel über das Internet. Bei der Community Cloud ist es hingegen möglich, darauf vollständig zu verzichten und über eigene Netzanbindungen der Teilnehmer den Zugang zu regeln. Das funktioniert meist per IPSec verschlüsselte Virtuelle Private Netzwerke (VPN) oder Multi-Protocol Label Switching (MPLS). Das Internet nicht einzubeziehen, bedeutet eine potenzielle Gefahrenquelle auszuklammern, die als Einfallstor für Malware und Attacken dient. Die direkte VPN-Anbindung weist geringere Latenzzeiten und garantierte Verfügbarkeiten auf – und damit eine bessere Performance, was über SLAs sicherzustellen ist. Außerdem ist über ein

MPLS-VPN Quality of Service (QoS) realisierbar, sodass das gesamte Community-Netz Ende-zu-Ende kontrollierbar bleibt.

Die CA – Türsteher mit VIP-Liste

Zur Kontrolle der Cloud-Nutzer empfiehlt sich eine eigene Certificate Authority (CA). Die CA erstellt, verwaltet und prüft die von ihr an die einzelnen User oder Geräte ausgegebene Zertifikate. Darüber hinaus legt die CA Certificate Revocation Lists (CRL) an, also Sperrlisten für zurückgezogene Zertifikate. Allerdings kann eine CA nur so gut sein wie die Organisationsprozesse um sie herum. Auch hier gilt: je unabhängiger desto verlässlicher. Aus diesem Grund sollten Dienstanbieter und CA-Betreiber immer eine Gewaltenteilung anstreben. Die Zugriffskontrolle liegt dann nicht mehr beim Dienstanbieter sondern beim CA-Betreiber als unabhängige Stelle. Dieser sollte auch für das Überprüfen der von der Community festgelegten Sicherheitsstandards verantwortlich sein und Zugänge für neue Teilnehmer nur bei positiv ausfallenden Resultaten gewähren. Genau dies ist innerhalb einer einzigen Institution oder eines einzigen Unternehmens nicht zu gewährleisten.

Verschlüsselung ist ein Muss

Nur Verschlüsselung gewährleistet letztendlich, dass diejenigen Zugriff auf Daten haben, die dazu auch berechtigt sind. Verschlüsselung setzt an drei Stellen an: Beim Transport der Daten in den Datenträgern und Datenbanken sowie bei der Verarbeitung. Je länger die Schlüssel und je sicherer die Algorithmen sind, desto stärker und sicherer ist auch die Verschlüsselung. Der Haken daran: Je härter die Verschlüsselung ist, desto langsamer werden in der Regel auch die Systeme. Das stellt vor allem an den Echtzeit-Gebrauch hohe Ressourcenanforderungen.

Die Transportverschlüsselung erfolgt heute in der Regel per IPSec oder TLS mit 2048 Bit Schlüssellänge. Die entsprechenden SSL/TLS-Zertifikate sind beispielsweise wieder über die CA auszugeben und zu kontrollieren.

Die Verschlüsselung der Datenbank auf Block-Ebene ist beispielsweise über systemweit gültige Schlüssel zu realisieren. Diese Schlüssel werden in speziellen Schlüsselspeichern aufbewahrt. Empfehlenswerter ist das Erzeugen nutzerindividueller Schlüssel, die nach dem Abmelden wieder zerstört werden. Ein starkes Blockchiffre wie AES256 (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit gewährleistet in dieser Variante eine hohe Sicherheit.

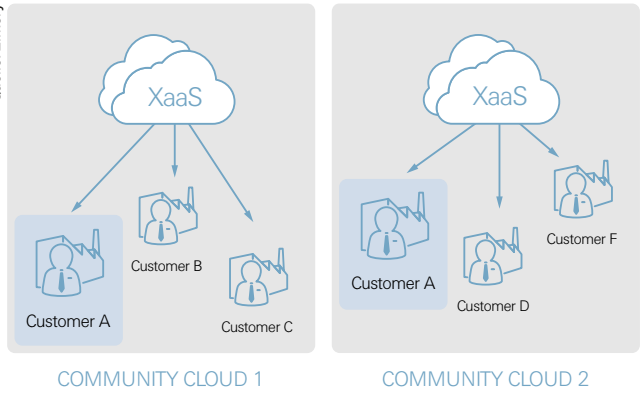
Selbstverständlich sollte der Cloud-Betreiber keinen Zugriff auf die Schlüssel der Clients beziehungsweise der Cloud-Nutzer haben. Nur so ist eine Vertraulichkeit der Daten gewährleistet. In der Regel sind es nicht gebrochene Algorithmen, die Sicherheitsprobleme verursachen, sondern Korruptionen der Umgebung oder der jeweiligen Implementierung.

Damit die Daten auch physisch sicher sind, werden sie in der Praxis häufig gesplittet, also auf unterschiedliche Rechner und Lokationen verteilt. Auf diese Weise ist sichergestellt, dass auch bei Diebstahl der Hardware die Cloud-Daten nicht vollständig in unbefugte Hände gelangen.

Alles im Gleichklang dank Standards

Die jeweiligen Nutzer einer Community Cloud bringen in der Regel unterschiedliche Voraussetzungen ihrer eigenen IT-Infrastruktur mit und verwenden unter Umständen zusätzlich eigene Private Clouds. Werkzeuge zur Cloud Orchestration, wie sie unter anderem Citrix, IBM oder Zimory anbieten, helfen beim Harmonisieren heterogener IT-Landschaften. Gleichzeitig unterscheiden sie zwischen den Private- und Community-Cloud-Ressourcen und bieten den einzelnen Usern einen getrennten Überblick über die genutzten Kapazitäten.

Quelle: Zimory



Anwender können prinzipiell auf mehrere Community Clouds zugreifen (Abb. 2).

Hier sind Standards wichtig, denn ohne diese sind Kompatibilität und Übertragbarkeit virtueller Maschinen und Datenformate in keiner Weise gegeben. Gleiches gilt für das Management der Cloud-Ressourcen genauso wie für Datensicherheit und Datenschutz oder für einheitliche SLAs. In diesem Kontext spielen vor allem zwei Standards eine wesentliche Rolle, Openstack und CIMI. Hersteller, die auf offene Strukturen und offene APIs setzen, bauen ihre Lösungen auf beiden Standards auf.

Zu den weltweiten Organisationen und Institutionen, die sich um die Cloud-Standardisierung bemühen, gehört auch die Distributed Management Taskforce (DMTF), der inzwischen 200 Unternehmen angehören. Sie hat die international erste standardisierte Management-Schnittstelle für virtuelle Maschinen verabschiedet, das Cloud Infrastructure Management Interface (CIMI). Diese Spezifikation beschreibt Modell und Protokoll, die Management und Interaktion zwischen den Clouds sowie zwischen dem Provider und dem Nutzer regeln. CIMI bezieht sich in erster Linie auf IaaS, ist aber auch für PaaS oder SaaS nutzbar. OpenStack beschreibt ein Cloud-Software-Projekt, das eine freie Architektur für Cloud Computing unter der Apache Lizenz bereitstellt. Diverse Firmen unterstützen das Projekt wesentlich, beispielsweise Citrix, Dell, HP, Redhat und IBM.

Open-Source-Lösungen mit CIMI und OpenStack haben nicht nur hinsichtlich der Standardisierung wesentliche Vorteile. Aus Security-Sicht ermöglichen sie im Gegensatz zu vielen proprietären Modellen eine umfangreiche Überprüfung der jeweiligen Sicherheitslösung. Open-Source-Standards gewährleisten darüber hinaus die Abstraktion unterschiedlicher APIs, sodass für ein Unternehmen notwendige Spezial-Funktionalitäten darüber abzubilden sind.

Gerade bei der Zusammenarbeit verschiedener Partner bietet sich ein Orchestration Tool an, da es eine einheitliche Plattform erzeugt. Es ermöglicht das Etablieren von Prozessstandards innerhalb der Community Cloud und erleichtert damit die Zusammenarbeit untereinander. Insgesamt gesehen bergen Community Clouds das Potenzial innerhalb einer Partnergruppe verschiedene Prozess- und Sicherheitsstandards zu etablieren und langfristig – auch über nationale Grenzen hinweg – durchzusetzen.

Josef Glöckl-Frohnholzer,
Managing Director, Zimory