Security im Cloud Computing

Die sichere Wolke

Sicherheit ist ein zentraler Faktor, wenn es um die Entscheidung geht, ob man Dienste und Anwendungen aus der Cloud beziehen soll. Trotz der zahlreichen Vorteile, die das Cloud Computing bietet – vor allem Kostenersparnis und Flexibilität – sind die Vorbehalte vieler Firmen, unternehmenskritische Anwendungen auszulagern, noch immer groß.

Wie beim klassischen IT-Outsourcing unterliegen auch Cloud-Services bestimmten Sicherheitsanforderungen, insbesondere dann, wenn sensible oder personenbezogene Daten verarbeitet werden. Für die Umsetzung und Einhaltung der gesetzlichen Datenschutzbestimmungen ist der Nutzer eines Cloud-Services verantwortlich, auch wenn er die Dienstleistung eines externen Providers in Anspruch nimmt. Für deutsche Unternehmen ist ohnehin gemäß Bundesdatenschutzgesetz (BDGS) eine Auftragsdatenverarbeitung grundsätzlich nur in der EU und im Europäischen Wirtschaftsraum möglich. Die in Deutschland besonders hohen Anforderungen an den Datenschutz veranlassen Unternehmen zunehmend, ihre Daten in deutsche Rechenzentren auszulagern, da diese dem BDSG entsprechen müssen.

Dem Auftraggeber muss bekannt sein, in welchen Staaten der Provider die Server betreibt und welchen gesetzlichen Regelungen sie damit unterliegen. Dies ist aber gerade im Falle von Public Clouds nicht immer zu gewährleisten. Die Public Cloud ist öffentlich, Benutzer teilen sich die zugrunde liegende Infrastruktur. Die Ressourcen, die ein IT-Dienstleister zur Verfügung stellt, lassen sich von unterschiedlichen Orten aus zentral über das Internet abrufen.

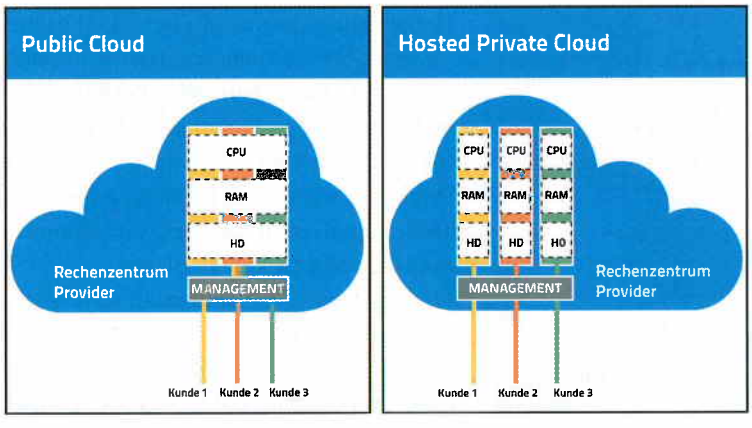
Eine Hosted Private Cloud hingegen steht nur einem einzelnen Unternehmen zur Verfügung. Sie bildet ein geschlossenes Netzwerk von IT-Ressourcen, Zugang zu ihr kann nur für autorisierte Personen, in der Regel über ein Intranet oder ein Virtual Private Network (VPN), erfolgen. Externe Dienstleister stellen Hosted Private Clouds zur Verfügung. Kommen mehrere Cloud-Infrastrukturen (Private und Public Cloud), die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam zum Einsatz, spricht man von einer Hybrid Cloud. Hybrid Clouds bieten die Möglichkeit, bestimmte Anwendungen in der am besten dafür geeigneten Umgebung zu betreiben.

Unabhängig davon, für welches Cloud-Modell sich ein Anwender entscheidet, muss er prüfen, ob das nationale Datenschutzrecht, dem seine Daten unterliegen, eine konforme Datenverarbeitung durch den Cloud-Anbieter zulässt. Der Cloud-Anbieter ist seinerseits verpflichtet, alle notwendigen organisatorischen und technischen Maßnahmen für die Informationssicherheit und den Datenschutz zu treffen. Ziel ist es dabei, die zur Verfügung gestellten Ressourcen vor unautorisierten Zugriffen zu schützen und – bei der Nutzung einer gemeinsamen IT-Infrastruktur – für eine sichere Isolierung der Mandanten zu sorgen.

Sicherheitstechnische Maßnahmen

Aus technischer Sicht ist für die Sicherheit der Rechenzentren, der Daten, der Plattformen und der Administration zu sorgen. Die RZ-Sicherheit bildet dabei die Basis der Architektur. Zu den wichtigsten Kriterien bei der Ausstattung des Rechenzentrums zählen eine redundante und unterbrechungsfreie Stromversorgung, redundante Klimatechnik, redundante Netzwerkinfrastruktur, Brandschutz, Videoüberwachungsanlagen, Sicherheitspersonal und mehrstufige Zugangskontrollen. Alle beschriebenen Komponenten sollten einer 24×7-Überwachung unterliegen.

Der Cloud-Service ist im Idealfall so ausgerichtet, dass jeder Kunde dedizierte Systemressourcen erhält, also die Möglichkeit, auf einen eigenen Storage-Bereich, eigene Ressourcen wie CPU und RAM und vor allem auf eine dezidierte Netzwerkinfrastruktur (VLAN) zugreifen zu können, um ein Höchstmaß an Performance und Sicherheit zu erhalten. Das Management-Netz des Cloud-Services ist dabei strikt vom Datennetz zur trennen. Die Cloud-Architektur sollte also getrennte Datenpfade für die Administration einerseits und die Anwendungen andererseits vorsehen. Bei der den Cloud-Services zugrunde liegenden Virtualisierung steuern Hypervisors den Zugriff auf gemeinsam genutzte IT-Ressourcen. Angriffe auf die Cloud-Infrastruktur sollten daher durch



Hosted Private Clouds unterscheiden sich von Public Clouds durch den Einsatz von dedizierten statt Shared-Ressourcen. Bild: Kamp Netzwerkdienste

Security-Systeme wie Firewalls und Antivirenprogramme besonders geschützt sein. Um die vereinbarten Leistungen und Maßnahmen überprüfen zu können, ist es notwendig, dass über Web-Schnittstellen oder APIs Kontrollen seitens des Nutzers stattfinden können. Es gibt entsprechende Tools, die umfassende Monitoring-Informationen über die Performance der genutzten Dienste liefern. Oft müssen Unternehmen diese Features jedoch zusätzlich zum Cloud-Service buchen.

Cloud-Services, die über ein Web-basiertes Interface administriert werden, müssen über einen sicheren Kommunikationskanal erreichbar sein. Das kann beispielsweise via VPN, TLS/SSL, IPSec, SSH oder eine Punkt-zu-Punkt-Verbindung erfolgen. Neben der sicheren Verbindung ist es wichtig, den Zugang zu kritischen Anwendungsbereichen durch starke Authentisierung zu schützen. Zwei-Faktor-Authentisierungen, wie sie etwa der Einsatz eines Security-Tokens bietet, sollten sowohl für die Administratoren des Cloud-Services als auch dessen Nutzer obligatorisch sein. Application Programming Interfaces (APIs) des Cloud-Services haben einen hohen Schutzbedarf und sollten für diejenigen, die keinen Zugriff benötigen, generell unerreichbar sein.

Daten, die der Benutzer in der Cloud abspeichert, sollten verschlüsselt sein (verschlüsselte Dateisysteme). Selbst bei einem physischen Zugriff auf die Dateisysteme bleiben so Inhalte und Informationen dem unberechtigt Zugreifenden verborgen. Auf der Ebene des Daten-Managements ist es nicht nur von Bedeutung, dass bei Nutzung eines gemeinsamen Datenspeichers die Kundendaten voneinander getrennt sind, sondern dass sie sich auch zuverlässig und unwiderbringlich löschen lassen. Eine Möglichkeit bietet hier das Überschreiben gelöschter Laufwerke. Eine Datenrekonstruktion auf Blockebene ist damit ausgeschlossen.

Um einer Abhängigkeit von einem Cloud-Anbieter vorzubeugen, sollte ein Unternehmen unbedingt im Vorfeld der Datenübertragung an den Provider eine Exit-Strategie festlegen. Neben dem Import von Appliances sollte es technisch möglich sein, angelegte Instanzen als Appliance zu exportieren und in andere Virtualisierungsumgebungen zu importieren.

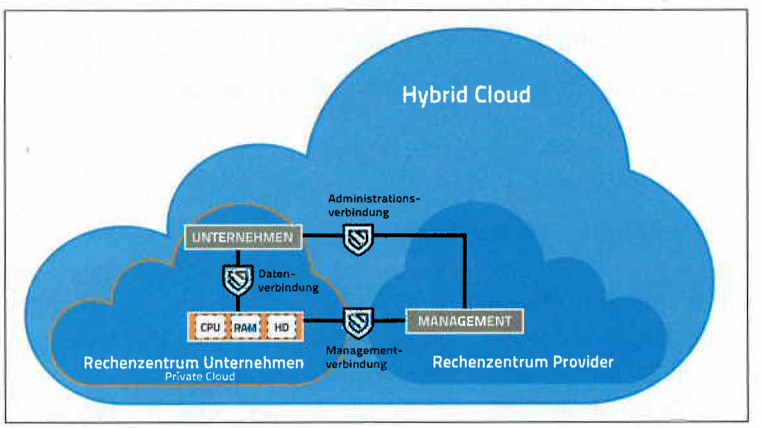
Individuelle Sicherheit in der Cloud

Unternehmen, die Daten mit einem höheren Schutzniveau auslagern wollen, sind auf ein Cloud-Modell angewiesen, das ihnen ein auf ihre spezifischen Anforderungen zugeschnittenes Sicherheitskonzept bietet. Dieser individuelle Lösungsansatz lässt sich am besten mit einer Hosted Private Cloud realisieren. Voraussetzung dafür ist, dass der Provider entsprechende Sicherheitsmaßnahmen umsetzt. Ein enger, vertrauenswürdiger Kontakt zum Anbieter ist wünschenswert. Es sollte ein persönlicher Ansprechpartner zur Verfügung stehen, um transparent die Rahmenbedingungen und SLAs zwischen Benutzer und Anbieter zu definieren. Hilfreich kann es sein, das Rechenzentrum des Cloud-Anbieters im Vorfeld zu besichtigen.

Im Gegensatz zur Private Cloud, bei der das Unternehmen selbst den hohen Aufwand für die Installation und Administration der Cloud hat, bietet die Hosted Private Cloud den Vorteil, dass der Provider die kontinuierlichen Investitionen in aktuelle Hardware und Technik sowie in das fachliche Know-how trägt.

Die Public Cloud wiederum zielt auf hohe Skalierbarkeit und Flexiblität und ist aus wirtschaftlicher Sicht äußerst attraktiv. Allerdings sind die Ressourcen hier nicht eindeutig lokalisierbar, damit die Daten nicht zu kontrollieren. Public-Cloud-Services stellen nur ein standardisiertes Sicherheitsmodell zur Verfügung, das für alle Cloud-Kunden bindend ist. Die Frage nach der Sicherheit in der Cloud lässt sich hier nicht allein durch technische Lösungen beantworten. Letztlich entscheiden genauso Compliance-Vorschriften und juristische Anforderungen darüber, ob man Daten und Dienste in eine Public Cloud auslagern kann.

Für die Hybrid Cloud gilt, dass für die relevanten Schnittstellen zwischen klassischer IT, Private und Public Cloud zusätzliche Schutzmechanismen implementiert sein müssen, um einen angemessenen Schutz und eine notwendige Trennung zwischen den Benutzern der Infrastrukturen zu gewährleisten. Kann die Hybrid Cloud ähnlich wie die Hosted Private Cloud individuell auf den Cloud Nutzer zugeschnitten werden, dann lassen sich auch hier IT-Ressourcen sicher nutzen.



Eine reizvolle Variante ist die Steuerung einer Hybrid Cloud mittels beim Provider gehosteter Software, während Server und Storage im RZ des Kundenunternehmens verbleiben. Bild: Kamp Netzwerkdienste

Mittlerweile gibt es auch Hybrid-Cloud-Modelle, die einen ganz neuen Ansatz verfolgen: Durch die Trennung der Cloud-Ressourcen von der Cloud-Steuerung verbleiben unternehmenskritische Daten auf der Hardware im eigenen Unternehmen, während lediglich die Steuerung der Cloud über eine zentrale Management-Plattform erfolgt, die ein Provider hostet. Dies hat den Vorteil, dass für den Benutzer keine Kosten für den Betrieb und die Wartung des Administrations-Servers anfallen und sensible Daten das eigene Rechenzentrum nicht verlassen müssen. Der Benutzer behält somit jederzeit die Kontrolle über seine Daten. Roland Irle/wg

Roland Irle ist CTO und Projektleiter Virtual-Core bei Kamp Netzwerkdienste.