SONDERDRUCK - CLOUD COMPUTING

bitmi
Bundesverband
IT-Mittelstand e.V.

„Vorwort“

Liebe BITMi-Mitglieder,

als Schlagwort der Informationstechnik ist “Cloud Computing” derzeit ein viel diskutiertes Thema, auch wenn die genaue Bedeutung vielen ein Rätsel bleibt.

Was bedeutet Cloud Computing? Einfach ausgedrückt bedeutet es, dass Software und Rechenleistungen nicht mehr lokal vom User bzw. dessen Rechner umgesetzt werden, sondern die Rechenleistung bzw. die Nutzung in einem übergeordneten, ausgelagerten Netzwerk geschieht. Warum es mit einer „Wolke“ gleichgesetzt wird, ist einfach erklärt: zeichnet man ein derartiges Netzwerk, wird dieses als Wolke dargestellt.

Zusammen mit dem Spezialversicherer Hiscox und dem ITK-Versicherungsmakler contego haben wir uns diesem Thema angenommen, und einige interessante Hintergrundinformationen für Sie zusammengestellt. Welche Risiken Cloud Computing für Betreiber und Nutzer birgt, ist hier die zentrale Fragestellung.

Contego ist der Spezialist für Risiken von IT- und Telekommunikationsunternehmen und bietet Beitragsvorteilen und Leistungserweiterungen. Verbandsmitglieder profitieren von dem Fachwissen bei der Gestaltung von Versicherungslösungen und bei der Abwicklung von Schadenfällen.

Wir hoffen, Sie mit diesem Sonderdruck begeistern zu können. Selbstverständlich freuen wir uns auch über Rückmeldungen und Themenvorschläge für weitere Ausgaben. Diese senden Sie bitte an info@bitmi.de.

Viel Spaß beim Lesen!

Ihr Dr. Oliver Grün
Vorstand des Bundesverband IT

Dieser Sonderdruck entstand in Zusammenarbeit mit unseren Partnern:

contego ITK-Spezialmakler

HISCOX

Datenschutzverletzungen in der Cloud

David Navetta, Esq., CIPP
Partner, InfoLawGroup LLP

Mit dem Jahr 2011 zeichnet sich ab, dass Cloud Computing weit mehr als eine reine Modeerscheinung ist, und zunehmend zu einem allgegenwärtigen Computermodell wird. Cloud Computing bringt eine Vielzahl an Vorteilen wie Effizienz, unmittelbare Skalierbarkeit und Wirtschaftlichkeit. Diesen Vorteilen muss allerdings entgegengesetzt werden, dass Organisationen die Kontrolle über ihren IT-Betrieb verlieren können, wenn sie zur Bereitstellung ihrer entscheidenden Prozesse völlig von einem Cloud Provider abhängen. Welche Problematiken dieser Verlust an Kontrolle mit sich bringt wird ersichtlich, wenn man sich mit der Reaktion auf und Haftung für Datenschutzverletzungen in der Cloud befasst.

Datenschutzproblematik in der Cloud

Wenn ein Cloud-Kunde sensible Daten in die Cloud stellt, ist er komplett auf die Sicherheitsvorkehrungen und im Fall einer tatsächlichen Datenschutzverletzung auf die Notfallmaßnahmen des Cloud Service Providers angewiesen. Diese Situation bringt zahlreiche grundlegende Probleme mit sich.

Wessen ‚Interessen' haben Vorrang?

Tritt bei einer Organisation, die ihre eigenen Daten verwaltet, eine Datenschutzverletzung auf, so liegt es auf der Hand, dass diese Organisation in ihrem eigenen Interesse den Vorfall vordringlich untersucht und für Abhilfe sorgt. Sie hat die Kontrolle über ihre Systeme und die darin befindlichen Daten und kann die entsprechenden Maßnahmen zum Schutz ihrer Interessen und Begrenzung ihrer Haftung treffen. Doch wie sieht das in der Cloud aus? Wenn die Daten des Kunden durch eine Datenschutzverletzung beim Cloud Provider gefährdet werden, so decken sich dessen Interessen möglicherweise nicht mit denen seiner Kunden. In dem Maß, in dem der Service Provider potenziell haftbar ist, kann sein

Vorgehen bei einem Angriff von seinen eigenen Interessen geleitet werden.

Die Cloud-Kunden haben möglicherweise keine Kontrolle über oder keinen Zugang zu Systemen, die sie gewöhnlich dazu nutzen würden, eine Bedrohung der Datensicherheit zu untersuchen, zu belegen oder zu beheben. Service Provider könnten versucht sein, bestimmte Informationen von ihren Kunden fernzuhalten, um sich selbst zu schützen. Da in vielen Clouds dieselben Computer und Netzwerke darüber hinaus von mehreren Kunden genutzt werden, können die Provider manche von ihnen bevorzugt behandeln. Große, wichtige und lukrative Kunden erhalten möglicherweise im Fall einer Datenschutzverletzung Vorrang vor anderen, ‚weniger wichtigen' Kunden.

Notfallplanung in der Cloud

Eine weitere wichtige Problemstellung der Datensicherheit in der Cloud sind die Notfallpläne. Beim Beitritt zur Cloud sollten sich Kunden über die Notfallpläne ihrer Cloud Provider informieren, sodass sie wissen, wie man dort nach einer Datenschutzverletzung verfährt. Wann liegt eine Datenschutzverletzung vor? Welche Methoden und Technik können eingesetzt werden, um Sicherheitsbrüche zu verhindern und zu ermitteln? Wie können Sicherheitsverstöße vom Cloud Provider untersucht und nach welchen Kriterien können ernsthaftere Vorfälle eskaliert werden, um den entstehenden Risiken entsprechend bearbeiten zu können? Bei dieser Analyse sollten Unternehmen ihre eigenen Richtlinien heranziehen und sie mit den Richtlinien des Cloud Providers abgleichen, um eine Übereinstimmung zu gewährleisten. Es ist außerdem entscheidend, dass die Notfallverfahren von Provider und Kunde so nahtlos wie möglich ineinandergreifen. Die Notfallpläne des Service Providers sollten die wichtigsten Kontaktstellen des Kunden einbinden, sodass der Kunde mit den erforderlichen Informationen versorgt wird, um seine eigenen Notfallpläne auszulösen (wenn der Kunde über einen guten Notfallplan verfügt, wird dieser die Koordination und Kooperation des Service Providers bereits einbeziehen)..

Forensische Ermittlungen und eDiscovery in der Cloud

Eine dritte Herausforderung besteht in der Fähigkeit eines Kunden, eine forensische Ermittlung durchzuführen, wenn sein Cloud Provider eine Datenschutzverletzung erleidet. Bei einem betriebsinternen Angriff könnte der Kunde ein Forensikunternehmen oder ein eigenes Team damit beauftragen, diesen zu untersuchen. Eine derartige forensische Ermittlung kann verschiedene Zwecke verfolgen, umfasst jedoch häufig die Analyse der Angriffsquelle und die Eliminierung von Eindringlingen. Man versucht herauszufinden, welche Daten betroffen sein könnten,

und abzuschätzen, wie sehr die Organisation exponiert wurde. Daneben werden Daten gesammelt und aufbewahrt, die zum Zweck der elektronischen Aufdeckung (eDiscovery) oder als elektronische Beweise bei Gerichtsverfahren dienen können.

Bei vielen Datenschutzverletzungen können forensische Ermittlungen von äußerster Wichtigkeit sein, beispielsweise um die Notwendigkeit und das Ausmaß der Benachrichtigungspflicht eines Unternehmens bei Verletzungen von personenbezogenen Daten zu ermitteln oder zu begrenzen. Bei einer forensischen Ermittlung gesammelte Informationen können zu Verteidigungs- oder Anklagezwecken im Prozessfall ausschlaggebend sein. Wurde beispielsweise der Schutz von Kreditkartendaten verletzt, so muss dieser Vorfall möglicherweise durch einen von VISA oder Mastercard ernannten Prüfer untersucht werden: andernfalls könnten diese Institute erhebliche Geldstrafen verhängen, und dem Kunden verweigern, zukünftig Kreditkarten zur Zahlung anzunehmen. Falls ein Unternehmen darüber hinaus nicht in der Lage ist, für juristische Zwecke möglicherweise relevante Daten forensisch zu sammeln und zu verwahren, kann dies ihre Fähigkeit beeinträchtigen, sich vor Gericht zu verteidigen.

Forensische Ermittlungen erfordern gewöhnlich den physischen Zugang der Prüfer zu den angegriffenen Computern vor Ort. Zudem können die erforderlichen Maßnahmen zur forensischen Erfassung von Daten den Betrieb der Systeme unterbrechen oder einschränken.

In der Cloud erlaubt der Provider seinen Kunden nach einer Datenschutzverletzung jedoch nicht unbedingt den physischen bzw. dezentralen Zugang zu seinen Servern oder gar die forensische Ermittlung auf seinen Systemen. Da ihre Server von mehreren Parteien gemeinsam genutzt werden, sind manche Cloud Provider der Ansicht, dass die forensische Erfassung von Daten auf den Servern vertrauliche Informationen anderer Kunden offenlegen würde, und somit möglicherweise gegen abgeschlossene Vertraulichkeitserklärungen oder Datenschutzbestimmungen verstoßen bzw. die Verfügbarkeit der Systeme für andere Kunden beeinträchtigen könnte. Ein weiterer Grund für die Ablehnung forensischer Ermittlungen liegt häufig in der Tatsache begründet, dass nach einer Datenschutzverletzung mehrere Kunden gleichzeitig ihr Recht hierauf beanspruchen könnten. Darüber hinaus könnte ein Cloud Provider die Möglichkeiten seiner Kunden beschränken wollen, eine Datenschutzverletzung zu untersuchen, um seine eigenen Interessen zu schützen und seine potenzielle Haftbarkeit einzugrenzen. Dies ist eine äußerst problematische Situation.

Die Providerkette in der Cloud

In der Cloud ist es häufig der Fall, dass der Provider, mit dem ein Unternehmen einen Vertrag abschließt (der ‚direkte Provider'), nicht der Cloud Provider ist, der die Daten des Kunden tatsächlich verarbeitet, speichert und überträgt (der ‚Drittprovider'). Das klassische Beispiel ist der Software-as-a-Service-Provider, der seine Software in einer Infrastructure-as-a-Service Cloud hostet. Bei einer derartigen Konstellation besteht möglicherweise keine Vertragsbeziehung zwischen dem angegriffenen Drittprovider und dem Cloud-Kunden, und dieser hat möglicherweise im Fall einer Datenschutzverletzung keine direkten Rechtsanspruch gegenüber dem Drittprovider. Da zwischen Drittprovider und den Cloud-Kunden eine oder sogar mehrere andere Parteien stehen, kann es schwierig sein, die Reaktionsfähigkeit nachgeschalteter Provider zu ermitteln. Hat der direkte Provider überdies vertraglich bestimmte Maßnahmen im Fall einer Datenschutzverletzung zugesagt, sich aber nicht die entsprechenden Rechte beim Drittprovider gesichert, so kann er seine Versprechungen womöglich nicht erfüllen. Darüber hinaus können in derartigen Konstellationen auch die bereits zuvor erörterten Interessenskonflikten auftreten und der Zugang für forensische Ermittlungen zusätzlich erschwert werden. Wenn es bereits schwierig ist, bei einem direkten Provider, mit dem man einen Vertrag abgeschlossen hat, Zugang zu erhalten, so kann dies praktisch unmöglich werden, wenn der Kunde keine Vertragsrechte hat.

Cloud-Vertrag und Datenschutzverletzung - was nun?

Wie kann ein Cloud-Interessent diesen Herausforderungen begegnen? Ist ein guter Vertrag nützlich? Die Antwort darauf lautet natürlich ‚Ja': Das Vereinbaren vertraglicher Rechte könnte zur Lösung derartiger Fragen äußerst hilfreich sein. Dabei sei jedoch betont, dass getroffene Absprachen von einem umsichtigen Due-Diligence-Prozess unterstützt werden müssen, um sicherzustellen, dass der Cloud Provider im Fall einer Sicherheitslücke tatsächlich seine Zusagen einhalten und die versprochenen Notfallmaßnahmen durchführen kann. Im Fall einer Datenschutzverletzung darf sich nicht herausstellen, dass ein Provider nur leere Versprechen abgegeben hat. Cloud-Kunden sollten die Aufnahme folgender Vertragsklauseln zur Absicherung bei Datenschutzverletzungen anstreben:

Notfallverfahren: Der Cloud-Kunde sollte versuchen, den Cloud Provider vertraglich dazu zu verpflichten, bestimmte Verfahren einzuhalten. Diese Verfahren sollten den eigenen Notfallmaßnahmen des Kunden entsprechen oder sich in diese eingliedern. So können u. a. insbesondere folgende Notfallpflichten festgelegt werden:

- Der sofortige Beginn von Ermittlungen nach einem Angriff;

- Schadensbegrenzung und Schließen von Sicherheitslücken; prompte Verständigung des Kunden (innerhalb von Stunden);
- Erstellen schriftlicher Berichte und Statusmeldungen über den Vorfall;
- Aufbewahrung relevanter Informationen über die Datenschutzverletzung (einschließlich Protokolle, Planungsunterlagen, Audit-Trails, Aufzeichnungen und Berichte)
- Dokumentieren von Gegenmaßnahmen.

Datenaufbewahrungspflicht: Im Falle eines Angriffs oder drohender gerichtlicher Verfahren kann es erforderlich sein, die relevanten Daten aufzubewahren (‚Litigation Hold' bzw. Datensicherung für Prozesszwecke). Der Cloud Provider sollte vertraglich dazu verpflichtet werden, im entsprechenden Fall eine derartige Datensicherung zu veranlassen. Der Kunde sollte außerdem versuchen, das Recht zu sichern, die Systeme des Cloud Providers eigenen forensischen Ermittlungs- und Sicherungsverfahren unterziehen zu können.

Das Recht auf forensische Untersuchung: Der Cloud-Kunde sollte versuchen, das Recht zu sichern, im Falle eines erfolgreichen Angriffs beim Cloud Provider eine eigene forensische Ermittlung durchführen zu können. Ist dies nicht möglich, so sollte das Onus auf den Cloud Provider übertragen werden, der darüber hinaus verpflichtet werden sollte, Berichte und Informationen über den Angriff bereitzustellen.

Beschränkungen für Cloud-Drittprovider: Die Nutzung von Dritten zur Bearbeitung, Speicherung und Weiterleitung von Daten durch den Cloud Provider kann vertraglich eingeschränkt werden. Es können entsprechende Bestimmungen aufgenommen werden, die einen Cloud Provider daran hindern, ohne vorheriges Einverständnis des Kunden Daten an andere Dienstleister weiterzugeben. Werden Dritt-Provider herangezogen, so kann der Service Provider vertraglich zu einem Due-Diligence-Verfahren verpflichtet werden, um sicherzustellen, dass der Dritt-Provider die mit dem direkten Provider vereinbarten Pflichten erfüllen kann. Daneben kann der Cloud-Kunde den Cloud-Provider auch vertraglich dazu verpflichten, Dritt-Providern ähnliche Pflichten wie die eigenen aufzuerlegen, sodass der direkte Provider seinen eigenen Pflichten nachkommen kann. Durch die Einbeziehung derartiger Vertragsbestimmungen erhalten Cloud-Kunden mehr Kontrolle und einen größeren Reaktionsspielraum bei Datenangriffen auf Dritt-Provider.

Verlustrisiko bei Datenangriffen: Letztendlich sind diejenigen Vereinbarungen am wichtigsten, die definieren, welche Partei bei einem Angriff auf den Serviceprovider den Verlust trägt. Die Vertragsbestimmungen sollten

definieren, dass das Verlustrisiko auf dem Cloud Provider liegt, beim dem der Datenschutz verletzt wurde. Dies kann in Form einer Entschädigungsklausel erfolgen, gemäß welcher der Cloud Provider den Kunden für alle aus der Datenschutzverletzung entstehenden Ansprüche und Verluste schadlos hält. Es kann ebenfalls bestimmt werden, dass der Cloud Provider dem Kunden im Fall einer Datenschutzverletzung entstandene Kosten beispielsweise Benachrichtigungen, Rechtsberatung, Postversand, Kreditkontrolle und Callcenter ersetzen muss. Die Kunden sollten auch Klauseln für Haftungsbeschränkung und Ausschluss von Folgeschäden eingehend prüfen und gegebenenfalls abändern. Derartige Klauseln begrenzen die Haftung des Service Providers für Datenschutzverletzungen, und Cloud-Kunden wollen möglicherweise eine unbegrenzte Haftung für Datenschutzverletzungen oder zumindest höhere Haftungsgrenzen anstreben. Alle Datenschutzpflichten müssen für den Fall einer Vertragsverletzung sorgsam formuliert werden. Ein Mangel an aussagekräftigen Haftungsklauseln kann die Auferlegung entsprechender Pflichten von vornherein unwirksam machen.

Fazit

Der Eintritt in die Cloud und die damit verbundenen Aufgaben der Kontrolle über die Datenverarbeitung, , ist eine schwerwiegende Entscheidung. Die mit Verletzungen des Datenschutzes einhergehenden Probleme zeigen die Herausforderungen, denen sich Cloud-Kunden bei Pannen im Cloud-Umfeld gegenübersehen. Vor der Entscheidung, mit einem Cloud Provider zusammenzuarbeiten, ist eine tief gehende Analyse der Risiken unumgänglich. Sind die Risiken vertretbar, so müssen sie trotzdem unbedingt vertraglich geregelt werden. Unternehmen, die rein vom Preis getrieben in die Cloud gehen und ein beträchtliches Maß an Kontrolle aufgeben, können bei Datenschutzverletzungen schnell Schiffbruch erleiden.

Aspekte der Risikoverteilung und -begrenzung in der Cloud

Dr. Carsten Schulz,
Taylor Wessing, Hamburg

Unter Cloud Computing versteht man die Zurverfügungstellung von Applikationen, Hardware und Systemsoftware durch Provider über das Internet. Dies ermöglicht den Kunden, IT-Ressourcen ihrem jeweiligen Bedarf entsprechend zu nutzen und den Umfang dieser Services rasch ihren eigenen Anforderungen anzupassen.

Aus dem Blickpunkt des Kunden betrachtet ist dies eine radikale Verlagerung des IT-Betriebs von einem infrastrukturbasierten Modell zu einem servicebasierten Ansatz. IT-Ressourcen werden damit ähnlich wie Strom, Wasser und andere Versorgungsleistungen auf Abruf verfügbar. Diese Verlagerung ist mit gravierenden Auswirkungen für die Einschätzung und Handhabung von IT-Risiken verbunden.

In der „Cloud“ angebotene IT-Services vareieren vom Outsourcing zentraler Unternehmensprozesse zur Bereitstellung relativ einfacher Verbraucherdienste wie Web-E-Mail. Dieser Artikel befasst sich ausschließlich mit ersterem.

Das traditionelle Risikomodell

Die mit dem Betreiben von IT-Infrastrukturen verbundenen Risiken sind hinreichend bekannt und umfassen u.a. Verfügbarkeit der Infrastruktur, Daten und Prozesse; Integrität der Infrastruktur; Datenschutz und Authentizität sowie Kommunikationssicherheit.

Sofern die IT-Infrastruktur unternehmensintern betrieben wird, bleiben Risikoanalyse und -management (einschließlich Risikovermeidung, -verringerung, -minderung, Risikoschutz und Versicherung) ausschließlich dem die IT-Ressourcen nutzenden Unternehmen vorbehalten. Typischerweise versuchen sich Unternehmen über Wartungsverträge und Lizenzvereinbarungen mit

Drittfirmen und Versicherungspolicen abzusichern, um diese Risiken zu managen.

Das Cloud-Risikomodell

Werden die IT-Prozesse allerdings in Form von Services aus der Cloud bezogen, verändern sich die entstehenden Risiken sowie ihre gesamte Strukturierung beachtlich.

- Einerseits werden spezifische Risiken beträchtlich reduziert, da spezialisierte Cloud Provider in der Lage sind, hochkarätige IT-Sicherheit, Business Continuity und Notfallplanung anzubieten.
- Gleichzeitig erwachsen allerdings neue Risiken in Form von Exit Management und Überleitung nach Ablauf eines Cloud Services Vertrags oder für den Zugang zu Daten und Systemen bei Insolvenz des Cloud Providers.

Daneben werden auch andere Risikomanagementmechanismen eingesetzt. Anstelle einer direkten Kontrolle von Beschäftigen und Infrastruktur werden bestimmte Service Level vereinbart, die die Bewertung und Überwachung der Servicequalität ermöglichen.

Obgleich sie für Risikoanalyse und -bewertung, das Erarbeiten von Vermeidungs- und Minimierungsstrategien sowie die Verteilung von Restrisiken und Ermittlung effektiver Überwachungs- und Kontrollmaßnahmen ausschlaggebend sind, lassen Kunden bei der Migration in die Cloud diese fundamentalen Risikoverlagerungen häufig außer Acht.

Beim Bereitstellen bzw. Erwerb von Cloud Services kann die Risikoverteilung auf verschiedenen Ebenen erfolgen, insbesondere:

- In der konkreten Gestaltung der Dienste, d. h. in der sachgerechten Zuweisung von Einflussbereichen und Risikoüberwachungsmechanismen; beispielsweise der Abstraktionsebene, auf der Dienste bereitgestellt/erworben werden (Infrastruktur als Service; Plattform als Service; Software als Service);
- durch die gesetzliche Risikoverteilung (insbesondere hinsichtlich der gesetzlichen Haftungsbestimmungen) sowie
- durch vertragliche Vereinbarungen als Hauptinstrument zur Korrektur und Anpassung der tatsächlichen und gesetzlichen Verteilung der Risiken.

Cloud Verträge

Cloud Services werden häufig in einem beträchtlichen Maß standardisiert, sowohl aus technischen Gründen (Nutzung derselben Plattform/Infrastruktur) als auch in der Absicht, eine effizientere Administration zu ermöglichen und die Transaktionskosten zu senken. Eine derartige Beziehung wird häufig

durch standardisierte Verträge bzw. zumindest durch grundlegende standardisierte Service-, Support- und Lizenzbedingungen geregelt, in denen die zu erbringenden Leistungen, Service Level, Verfügbarkeit und Rechtsmittel festgelegt sind. Wird die Bewertung und Verteilung der Risiken in diesen, einem langfristigen Vertragsverhältnis gewöhnlich zugrunde liegenden Standardverträgen/Service-Rahmenverträgen nicht von Anfang an entsprechend berücksichtigt, so kann das in der Folge zu einer problematischen Aggregation von Problemen und Risiken beim Cloud Provider führen, die wiederum bestimmte Versicherungsimplikationen mit sich bringt.

Der Einfluss des deutschen Rechts auf Cloud Verträge

In Deutschland stellen sich für standardisierte Cloud Services hinsichtlich der vertraglichen Verteilung der Risiken spezielle Problematiken, da hier die Formulierungsfreiheit der Allgemeinen Geschäftsbedingungen der Vertragsparteien von Gesetzesseite bereits erheblich eingeschränkt ist. Wie bereits zuvor für standardisierte Leistungen dieser Art erläutert, ist eine standardisierte Vertragsgestaltung gleichermaßen angebracht und erforderlich. Werden Standardprodukte auf derselben Plattform angeboten, so bleibt wenig Spielraum für eine abweichende vertragliche Risikoverteilung bei verschiedenen Kunden.

Eine entscheidende Hürde ist jedoch, dass die deutschen Gesetze zur Gestaltung Allgemeiner Geschäftsbedingungen eine freie Risikoverteilung zwischen den Vertragsparteien nicht zulassen, und darüber hinaus bestimmte Haftungsbeschränkungen der Provider (wie sie häufig in anderen Ländern angewandt werden) unterbinden. Folglich sind einer maßgeschneiderten Vertragsgestaltung zwischen Providern und Kunden enge Grenzen gesetzt.

Damit ist es allerdings noch nicht getan: Ist eine Bestimmung der Allgemeinen Geschäftsbedingungen nicht mit den gesetzlichen Vorschriften konform, so wird diese Vorgabe dadurch vollständig unwirksam und stattdessen die gesetzliche Bestimmung gültig. Dies hat folgende Konsequenzen:

1. Nicht jede Verteilung der Risiken ist in standardisierten Absprachen zulässig; die Provider müssen bestimmte Risiken tragen, außer auf individueller Basis wird eine abweichende Regelung vereinbart.
2. Versuche, Risiken mittels Allgemeiner Geschäftsbedingungen unter den Parteien zu verteilen, können dazu führen, dass der Provider gezwungen wird, die unbegrenzte Haftung zu übernehmen, falls die Allgemeinen Geschäftsbedingungen nicht die strengen Richtlinien der geltenden Gesetzgebung erfüllen, was zweifellos nicht im Interesse des

Providers ist. Gleichzeitig ist es allerdings auch nicht unbedingt im Interesse der Kunden. Eine Verteilungsstruktur, durch die der Provider bestimmte Risiken nicht mehr kontrollieren kann, könnte zu Instabilitäten auf Systemebene führen und somit ein Risiko für alle Kunden dieses Providers darstellen.

Fazit

Risikovermeidung, Risikominderung, Risikoverteilung und Risikoschutz sind eng miteinander verbunden, und diese Wechselbeziehungen erschließen den Parteien eine Reihe von Möglichkeiten, unter Einbeziehung der jeweiligen Versicherungsträger für alle Beteiligten akzeptable Vereinbarungen zu erarbeiten.
Im klassischen Outsourcing (in vieler Hinsicht ein Vorläufer von Cloud Services) wurden gute Industriestandards und beste Praktiken etabliert, und dies wird wohl nun auch im Cloud Services Bereich geschehen.

Die wichtigsten versicherbaren Ereignisse und Verluste in der Cloud

Thomas Jansen, Partner, DLA Piper Munich
Mark O'Conor, Partner, DLA Piper London

Sollten sich Parteien bei Vertragsverhandlungen mit der Verteilung der Risiken befassen und fragen, wer welche Risiken tragen soll? Welche Verluste können durch bestimmte Ereignisse entstehen und wer sollte dafür aufkommen? Die Verteilung der Risiken kann beträchtliche Konsequenzen für die Haftung von Kunden und Cloud Provider und folglich wiederum für deren Versicherungsschutz haben. Bevor man die entsprechende Versicherungsart und ausreichenden Versicherungsschutz erwerben kann, muss man wissen, gegen welche Ereignisse und Verluste man sich versichern will.

Bei einem Cloud-Vertrag müssten so viele verschiedene Ereignisse und Verlustrisiken in Betracht gezogen werden, dass ihre Analyse und Bewertung den Rahmen dieses Beitrags bei Weitem übersteigen würde. Wir beschränken uns daher auf die Zusammenfassung der wichtigsten Ereignisse und Verluste und einiger geeigneter Vorgehensweisen. Alle Parteien, die eine Verlagerung in die Cloud erwägen, müssten ihre jeweilige Haftung bei bestimmten Ereignissen und Verlusten eingehender prüfen und ermitteln, in wie weit sie sich dagegen versichern könnten.

Ihr Cloud Provider macht Konkurs - wie können Sie Ihre Daten zurückerhalten und die Daten und Technologie einem anderen Anbieter übertragen?

- Von einem juristischen Standpunkt betrachtet besteht kein Unterschied zu den herkömmlichen Outsourcing-Konzepten.
- Der Vertrag muss entsprechende ‚Exitklauseln' enthalten, die die Rechte des Kunden sichern, die Daten zurückzuerhalten oder einem neuen Provider zu übertragen.
- Aus praktischer Sicht kann dies

schwierig werden, wenn der Cloud-Anbieter einen Drittprovider mit dem Hosting der Daten beauftragt hat. In diesem Fall sollte der Kunde berechtigt sein, die Daten vom Drittprovider zurückzufordern.

Ihr Cloud Provider überträgt Ihre Daten unerlaubterweise unter Verletzung der Datenschutzgesetze und anderer Regelungen

- Von einem juristischen Standpunkt betrachtet besteht kein Unterschied zu den herkömmlichen Outsourcing-Konzepten.
- Die relevanten Datenschutzmaßnahmen und -vorschriften müssen vertraglich festgelegt sein.
- Der Vertrag muss dem Kunden außerdem detaillierte Überwachungsrechte einräumen.
- Bei einer Vertragsverletzung muss der Kunden berechtigt sein, den Vertrag zu kündigen.
- Der Vertrag muss entsprechende ‚Exitklauseln' enthalten, die die Rechte des Kunden sichern, die Daten zurückzuerhalten oder einem neuen Provider zu übertragen.
- Sofern dem Kunden aufgrund einer Verletzung der Datenschutzgesetze durch den Cloud Provider behördliche Geldstrafen oder sonstige Ansprüche drohen, darf die Haftung des Cloud Providers für derartige Ansprüche nicht ausgeschlossen oder begrenzt sein.

Welche Maßnahmen können Sie ergreifen, wenn Ihr Cloud Provider mangelhafte Dienste leistet (in Anbetracht dessen, dass die Haftung bei ‚normalen' Cloud-Verträgen häufig begrenzt und kein Service Level Agreement enthalten ist)?

- Von einem juristischen Standpunkt betrachtet besteht kein Unterschied zu den herkömmlichen Outsourcing-Konzepten.
- Man muss zwischen "Public-Cloud-Services" und den "Private- oder Enterprise-Cloud-Services" unterscheiden.
- Public Cloud-Angebote sind eventuell nur für nicht kritische, unkomplizierte Standardanwendungen und -daten geeignet, da Verträge für public Cloud-Dienste keine kundenfreundlichen Gewährleistungs- und Service-Level-Bestimmungen aufweisen.
- Bei "Private- oder Enterprise-Cloud-Services" Angeboten ist dies meist anders. Derartige Dienste und Verträge sind gewöhnlich spezifisch auf einen bestimmten Kunden abgestimmt und enthalten meist die entsprechenden Gewährleistungs- und Service-Level-Zusagen.

Was ist, wenn der Provider keine ausreichenden Disaster-Recovery-Vorkehrungen trifft?

- Von einem juristischen Standpunkt betrachtet besteht kein

Unterschied zu den herkömmlichen Outsourcing-Konzepten.

- Disaster-Recovery-Vorkehrungen (einschließlich Backup-Vereinbarungen) müssen vertraglich festgelegt und vereinbart werden.
- Der Vertrag muss dem Kunden außerdem detaillierte Überwachungsrechte einräumen.
- Bei einer Vertragsverletzung muss der Kunden berechtigt sein, den Vertrag zu kündigen.
- Der Vertrag muss entsprechende ‚Exitklauseln' enthalten, die die Rechte des Kunden sichern, die Daten zurückzuerhalten oder einem neuen Provider zu übertragen.
- Sofern dem Kunden aufgrund einer Verletzung der Datenschutzgesetze durch den Cloud Provider behördliche Geldstrafen oder sonstige Ansprüche drohen, darf die Haftung des Cloud Providers für derartige Ansprüche nicht ausgeschlossen oder begrenzt sein.

Die Nutzung der Cloud ist abhängig vom verfügbaren Internetzugang. Was geschieht, wenn der grundlegende Netzwerkbetreiber ausfällt? Wer wäre in diesem Fall verantwortlich?

- Von einem juristischen Standpunkt betrachtet besteht kein Unterschied zu den herkömmlichen Outsourcing-Konzepten.
- Gewöhnlich besteht eine vertragliche Regelung zwischen dem Cloud Service Provider und dem Kunden einerseits und eine weitere vertragliche Regelung in Form eines Untervertrags zwischen dem Cloud Service Provider und dem Netzwerkbetreiber.
- In der Beziehung zwischen dem Cloud Provider und dem Kunden würde ein Ausfall des Netzwerkbetreibers als Ausfall des Cloud Providers betrachtet und folglich müsste der Cloud Provider den Kunden für alle durch das Ausfallen des Netzwerkbetreibers verursachten Verluste entschädigen.
- Sofern der Kunden für eine Verletzung der Datenschutzgesetze durch den Cloud Provider haftbar gemacht werden könnte, darf die Haftung des Cloud Providers für derartige Ansprüche nicht ausgeschlossen oder begrenzt sein.

Was geschieht bei einem Denial-of-Service-Angriff oder einer Datenschutzverletzung? Wer wäre in diesem Fall verantwortlich?

- Von einem juristischen Standpunkt betrachtet besteht kein Unterschied zu den herkömmlichen Outsourcing-Konzepten.
- Die relevanten Datenschutzmaßnahmen und -vorschriften müssen vertraglich festgelegt sein.
- Der Vertrag muss dem

Kunden außerdem detaillierte Überwachungsrechte einräumen.

- Bei einer Vertragsverletzung muss der Kunden berechtigt sein, den Cloud-Vertrag zu kündigen.
- Der Vertrag muss entsprechende ‚Exitklauseln' enthalten, die die Rechte des Kunden sichern, die Daten zurückzuerhalten oder einem neuen Provider zu übertragen.
- Sofern der Kunden für eine Verletzung der Datenschutzgesetze durch den Cloud Provider haftbar gemacht werden könnte, darf die Haftung des Cloud Providers für derartige Ansprüche nicht ausgeschlossen oder begrenzt sein

Fazit

Von einem juristischen Standpunkt betrachtet besteht kein großer Unterschied zwischen Cloud-Serviceangeboten und herkömmlichen Outsourcing-Konzepten.

Es gibt keine ‚marktüblichen' Standardvertragsbestimmungen, da der Markt noch in der Entwicklung begriffen ist, bestimmte Thematiken kristallisieren sich jedoch heraus. So sehen wir eine Taxonomie von Vertragsstilen, angefangen bei ‚neuen' Providern (Salesforce, Google, Amazon, Memset, Rackspace etc.), die versuchen, ihre Haftung möglichst oder sogar völlig auszuschließen, über traditionelle ‚alte' Marktteilnehmer (Cisco, Fujitsu, IBM etc.), die weniger geneigt sind, die Bedingungen ihrer Cloud-Verträge offenzulegen, hin zu Hybrid-Providern wie Microsoft, die für ihr Azure-System eingeschränkte Service Level und in IT-Verträgen üblichere Bestimmungen anbieten.

Billigere Technologie über die Cloud ist mit gewissen Kompromissen in puncto Sicherheit verbunden. Sie bekommen das, wofür Sie bezahlen! Die Entscheidung wird ebenso von der Notwenigkeit, Geld zu sparen, als von den Sicherheitsanforderungen der betroffenen Daten getrieben. So könnten beispielsweise nicht kritische Daten zu einem billigen Offshore-Cloud-Provider ausgelagert werden, der hinsichtlich Service Level oder Zuverlässigkeit nicht viel bietet, während sensible personenbezogene Daten vertraglich besser geschützt werden müssen.

Sie möchten Ihr Unternehmen schützen und eine spezielle IT-Versicherung abschließen?

Contego ist der Spezialist für Risiken von IT- und Telekommunikationsunternehmen und bietet Beitragsvorteile und Leistungserweiterungen. Verbandsmitglieder profitieren von dem Fachwissen bei der Gestaltung von Versicherungslösungen und bei der Abwicklung von Schadenfällen.

Für weitere Informationen kontaktieren Sie bitte:

bitmi
Bundesverband
IT-Mittelstand e.V.

Herr Rolf Chung

Bundesverband IT-Mittelstand e.V.
Augustastraße 78-80, 52070 Aachen

Telefon: +49 241 1890 558
Telefax: +49 241 1890 555
eMail: info@bitmi.de

contego ITK-Spezialmakler

Herr Jan Fries

Contego Finanzberatung GmbH
Maximlianstraße 43, 80538 München

Telefon: +49 89 550 648 50
Telefax: +49 89 550 648 55
eMail: jfries@contego.de