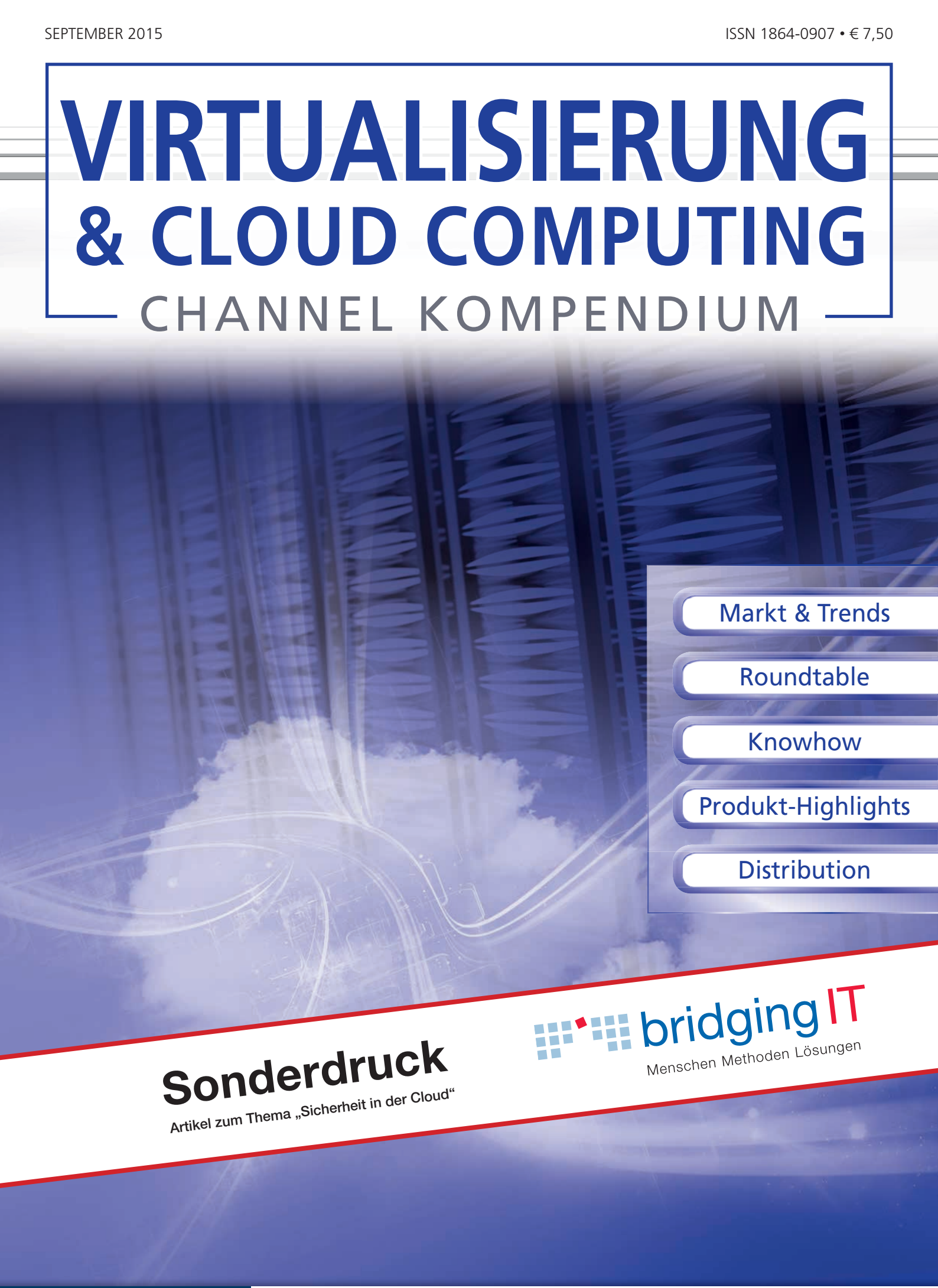
SEPTEMBER 2015

ISSN 1864-0907 • € 7,50

VIRTUALISIERUNG & CLOUD COMPUTING

CHANNEL KOMPENDIUM



- Markt & Trends
- Roundtable
- Knowhow
- Produkt-Highlights
- Distribution

Sonderdruck

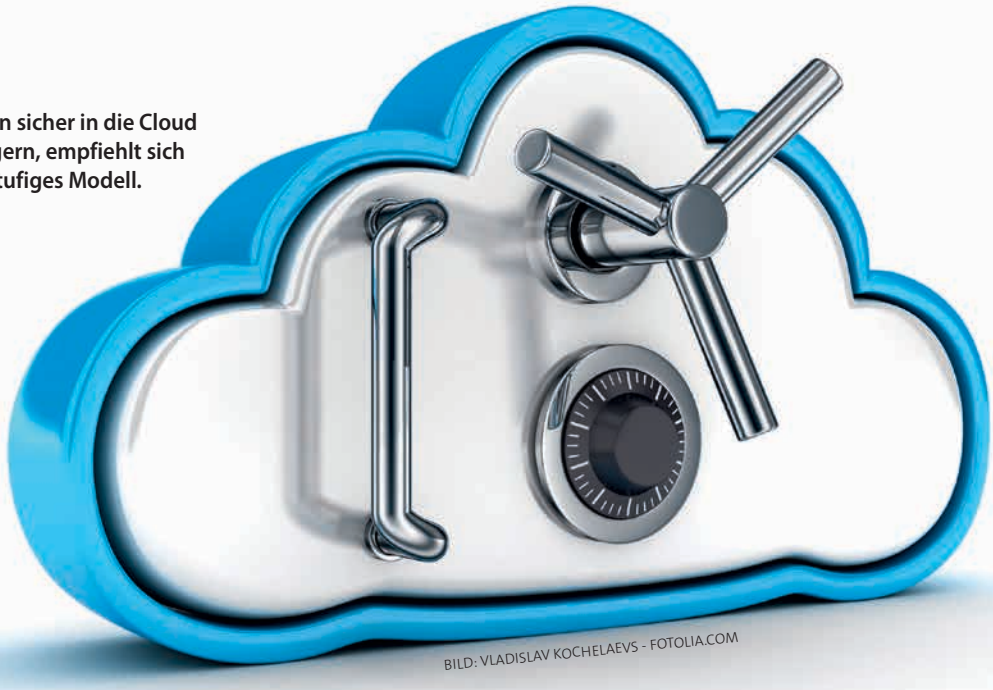
Artikel zum Thema „Sicherheit in der Cloud“

bridging IT

Menschen Methoden Lösungen

Vogel Business Media

powered by IT-BUSINESS



Um Daten sicher in die Cloud zu verlagern, empfiehlt sich ein vierstufiges Modell.

BILD: VLADISLAV KOCHELAEVS - FOTOLIA.COM

Services mit System

Sicherheit in der Cloud

Cloud Computing bedeutet nicht nur die Bereitstellung von IT-Ressourcen wie Server oder Speicher durch einen Cloud-Anbieter. Cloud Computing ist vielmehr ein Service-Modell, welches gewisse Grundbedingungen voraussetzt. Neben einer hohen Standardisierung des Services und einer weitgehenden Automatisierung bei der Bereitstellung verlangt es vor allem nach einem: Vertrauen!

von Dr. Jochen Ruben und David Schleweis

Das ist für die meisten Unternehmen erstmal schwer zu verinnerlichen, verbinden viele doch den Begriff „Service“ mit dem noch vorherrschenden klassischen Outsourcing. Hier ist man als Outsourcing-Nehmer seit Jahren gewohnt, seinem Dienstleister mit allerlei Bedingungen im Rahmen von SLAs die eigenen Qualitätsanforderungen vorzugeben. Ähnlich sieht es mit vertrauensschaffenden Maßnahmen wie einem Audit des Rechenzentrums aus. Hier ist es beim Outsourcing bislang üblich, dass sich der Dienstleister im Vertrag meist das Recht auf die Auditierung des Rechenzentrums beim Servicelieferanten einräumt.

Beides ist beim Bezug von Services aus der Cloud nicht möglich. Service-Bezieher müssen sich darauf verlassen, dass der Cloud-Anbieter seine Arbeit gewissenhaft und nach geltendem Recht macht. Vertrauen schaffen kann hierbei natürlich das Vorweisen von Zertifikaten unabhängiger Institutionen, welche die Anbieter und ihre Dienste in regelmäßigen Abständen auditieren. Wichtig ist hierbei auch die Einhaltung von internationalen Industriestandards wie ISO 27001, SOC 1-3 oder HIPAA.

Cloud Computing ist Vertrauenssache

Angesichts dieser Ausgangssituation zählt vor allem: Hat das Unternehmen Vertrauen zum Cloud-Anbieter gefasst oder nicht? Vor dem Hintergrund der Ausspähung durch Geheimdienste weltweit wird von der Unternehmens-IT immer wieder die Frage gestellt, wo das Schlüsselmaterial in der Cloud gespeichert wird und wer es nutzen kann. Hier hat sich der Einsatz von „High Secure“-Modulen (HSM) als geschütztem Speicherort innerhalb der Cloud bewährt. So verbleibt das Schlüsselmaterial in der Hoheit des Unternehmens und kann weder vom Cloud-Anbieter noch von einem Dritten genutzt werden. Damit lassen sich die Grundvoraussetzungen vieler Security-Richtlinien in Un- >

INFO

Mer Infos zu Cloud und Virtualisierung:

www.it-business.de, Partnerzone Virtualisierung

Zum Thema

ternehmen erfüllen. Darüber hinaus können es Sicherheits- oder Compliance-Vorgaben notwendig machen, dass die Verarbeitung und Speicherung von Anwendungen und Daten auf dedizierten physischen Servern und Speichersystemen erfolgen müssen. Auch dies sollte der Cloud-Anbieter ermöglichen. Zudem sollte er sicherstellen, dass kritische Daten auf Wunsch nur innerhalb der EU oder innerhalb Deutschlands verarbeitet, gespeichert und repliziert werden.

Welche Daten wohin?

Hat das Unternehmen grundsätzliches Vertrauen zum Cloud-Anbieter und dessen Standard-Servicemodell gefasst, stellt sich für die Entscheider die Frage nach der Kritikalität der auszulagernden Daten, und ob sie gegebenenfalls irgendwo innerhalb der Cloud des Providers verarbeitet, gespeichert und repliziert werden können. Für diese Entscheidung spielen die unternehmensinternen IT-Security-, IT-Compliance- und IT-Governance-Richtlinien eine entscheidende Rolle.

Speziell bei der Frage, welche Daten zur Sicherheit und zu Dokumentationszwecken innerhalb des Unternehmens verbleiben müssen und welche auch außerhalb verarbeitet und gespeichert werden können, hat sich in den letzten Jahren eine Klassifizierung in vier Stufen herauskristallisiert:

- **Streng vertraulich**
  Besonders kritische Daten wie Vorstands-, F&E- und Patentdaten sowie strategische Daten sollten innerhalb der eigenen IT auf besonders abgesicherten, gegebenenfalls von der Corporate Cloud abgeschotteten Servern und Speichersystemen verarbeitet und abgelegt werden.
- **Vertraulich**
  Andere kritische Daten können in eine Public Cloud ausgelagert werden, wenn der Dienstleister dem Unternehmen mit den zuvor beschriebenen vertrauensschaffenden Maßnahmen entgegenkommt und die IT-Sicherheits- und Compliance-Richtlinie des Unternehmens nichts anderes vorgeben.
- **Intern**
  Hierunter versteht man alle Daten, die weder vertraulich oder streng vertraulich und nicht öffentlich zugänglich sind. Sie können meist problemlos innerhalb der Cloud verarbeitet, gespeichert und repliziert werden.
- **Public**
  Diese Daten sind ohnehin bereits online frei zugänglich und daher unkritisch.

Zugriffssicherheit im eigenen Cloud-Umfeld

Eine besondere Herausforderung im Cloud-Umfeld stellt die Umsetzung einer umfassenden Zugriffskontrolle dar. Wenn Daten und Anwendungen losgelöst von bestimmten Servern und Speichern verarbeitet und abgelegt werden, muss die Kontrolle innerhalb der Wolke auf logischer Ebene erfolgen. Anforderungen wie Identity Management, Zugriffskontrolle und rollenbasierende Trennung von Verantwortlichkeiten („Separation of Duties“) haben die meisten Unternehmen bereits umgesetzt. Woran es vielerorts noch mangelt, ist ein internes Monitoring der administrativen Tätigkeiten. Weil Administratoren als privilegierte User weitgehende Berechtigungen haben, um beispielsweise Benutzerrechte für IT-Ressourcen einschließlich der Daten und Anwendungen zuzuweisen und sie zu konfigurieren, können von ihnen unmittelbar wie mittelbar hohe Risiken ausgehen: Datenausspähungen, Datendiebstahl, Manipulationen von Systemen, Anwendungen und Daten bis hin zur Sabotage kompletter Geschäftsabläufe. Daher sollten bei dieser Benutzergruppe die Berechtigungen auf das Notwendigste beschränkt und besonders granular vergeben werden. An der Analyse, was das Notwendige ist, sollte neben der IT-Abteilung unbedingt die Fachseite mitwirken. Die Fachverantwortlichen können am besten für ihren Bereich beurteilen und bewerten,

- welche Mitarbeiter mit welchem Tätigkeitsprofil über welche Endgeräte mit welchen IT-Ressourcen einschließlich der Daten und Anwendungen arbeiten,
- wie geschäftskritisch diese IT-Ressourcen für das Unternehmen sind,
- welche Berechtigungen und Konfigurationen für diese IT-Ressourcen eingeräumt werden müssen, um ihren Einsatz sicherzustellen und sie vor unberechtigten Zugriffen Dritter abzuschirmen.

Mit den Ergebnissen dieser Analyse können die Berechtigungen der Administratoren für jede Fachabteilung in Form von Administrationsrollen innerhalb des IAM-Systems (Identity and Access Management) hinterlegt und dadurch die Risiken und ihre teils drastischen Folgen minimiert werden. Diese Verfahrensweise trägt zudem auch zu einer besseren, revisionssicheren Nachvollziehbarkeit der administrativen Tätigkeiten bei.

Dr. Jochen Ruben, Portfolio-Line Manager für die Themen IT-Architektur, -Infrastruktur und -Betrieb bei bridgingIT

David Schleweis, Leiter des Center of Excellence Cloud Computing & Virtualisierung bei bridgingIT

bridging IT

Menschen Methoden Lösungen

BridgingIT GmbH
N7, 5-6
68161 Mannheim
Tel.+49 621 370 902 - 0
www.bridging-it.de

innovation@bridging-it.de