VDI nachrichten

Position

Seite 13
Rubrik

Kunde All for One Steeb AG

Ausgabe
04.07.2014/Nr. 27/2014

Medienart Printmedien
Medientyp Fachpresse
Erscheinungsweise wöchentlich
Branche Wirtschaft Allgemein
Bundesland Überregional
Nielsengebiet nicht zugeordnet

Auftrags-Nr. 13612
Kunden-Nr. 31272
Thema-Nr. 051.069

Suchbegriff(e) 1. All for One, -Steeb AG

Verlag VDI Verlag GmbH, 40468 Düsseldorf, VDI-Platz 1, Tel.: 0211 6188 0, Fax: 0211 6188 112
E-Mail: info@vdi-nachrichten.com, URL: www.vdi-verlag.de

Redaktion VDI Nachrichten Redaktion, 40468 Düsseldorf, VDI-Platz 1, Tel.: 0211 61880, Fax: 0211 6188112
E-Mail: redaktion@vdi-nachrichten.com, URL: www.vdi-nachrichten.com

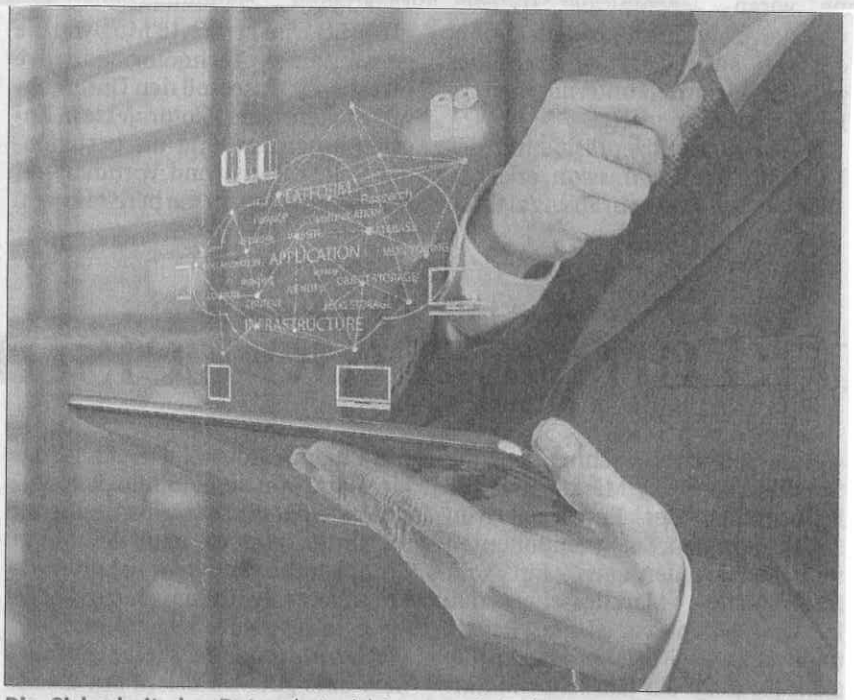
Publikation	Auflage * verkauft	verbreitet	gedruckt	Reichweite** (in Mio.)	Medien-Nr.
VDI Nachrichten	154.118	160.332	158.915 [1]	0,31 [a]	2204

Quelle(n): * 1. IVW ** a. AWA

„Am Ende ist Datensicherheit in der Cloud reine Verhandlungssache“

CLOUD-COMPUTING: Datensicherheit und Datenschutz sind zwei wesentliche Aspekte, die Firmen von Cloud-Anbietern erwarten. Deutsche Anbieter haben die Zeichen der Zeit erkannt und bieten ihren Kunden maßgeschneiderte Lösungen, von verschlüsselten Datenübertragungen bis zur Wahl der Datenaufbewahrung.

VDI nachrichten, Düsseldorf, 4. 7. 14, pek



Die Sicherheit der Daten hat nicht nur technische Komponenten. Mindestens ebenso wichtig ist die tägliche Umsetzung von Unternehmensregeln, um Datenlecks zu vermeiden. Foto: Everythingpossible/Fotolia

Spätestens seit den NSA-Enthüllungen wird das Thema Datensicherheit in der Öffentlichkeit intensiv diskutiert. Der Mittelstand hält sich seitdem hinsichtlich seines Interesses am Cloud-Computing deutlich zurück. Das konsequente Pochen auf die Einhaltung von Sicherheitsstandards lässt viele Firmen über die sichere Nutzung einer Private oder Managed Cloud nachdenken.

„Wir hosten unsere Cloud-basierten Lösungen explizit in deutschen Rechenzentren und können so unseren Kunden einen sicheren Ort für ihre sensiblen Daten gewährleisten“, versichert Martin Hubschneider, Vorstandsvorsitzender der CAS Software AG und stellvertretender Vorsitzender des IT-Mittelstandsverbandes BITMi.

Das Bundesdatenschutzgesetz und der Schutz der Persönlichkeitsrechte sowie verschiedene europäische Richtlinien würden von CAS Software eingehalten, es gebe keine Hintertürchen – für wen auch immer. „Sollte ein Geheimdienst an uns herantreten und Zugang zu Daten fordern, würden wir sofort alle Hebel in Bewegung setzen und Presse und Öffentlichkeit informieren“, verspricht Hubschneider.

SAP Deutschland, Pironet NDH, All for one Steeb und viele weitere Cloud-Anbieter, die ihren Sitz in Deutschland haben, sichern ihren Kunden ebenfalls die Einhaltung gesetzlicher Vorschriften zu.

„Aber woher weiß der Kunde, welche Sicherheitstechnologien beim Provider zum Einsatz kommen?“, fragt Holger Kisker, Analyst bei Forrester. „Daher muss die Dienstgütevereinbarung alles beinhalten, was dem Unternehmen bezüglich Sicherheit wichtig ist.“

Bei einem Public Cloud Angebot sei der Einfluss des Kunden wegen der hohen Standardisierung oft sehr eingeschränkt, daher böten sich für Bereiche, die spezielle Sicherheitsanforderungen haben, meist eher Managed-Cloud-Dienstleistungen an. „Am Ende ist alles Verhandlungssache“, meint Kisker

Das muss aber nicht so sein. „Wir bei AWS haben uns von Anfang an dazu entschlossen, unseren Kunden die Kontrolle zu geben“, sagt Martin Geier, Geschäftsführer Deutschland bei Amazon Web Services Germany (AWS). „Sie besitzen die Daten und sie entscheiden, wo sie gespeichert werden. Die Daten europäischer AWS-Cloud-Kunden verbleiben auch in Europa.“ AWS stelle Anwendern Werkzeuge und Techniken zur Verfügung, mit denen sich Daten verschlüsseln lassen, und zwar sowohl vor Ort als auch während der Übertragung. „Die geheimen Schlüssel werden so verwaltet, dass der Kunde die Kontrolle darüber behält, wer auf die Daten zugreifen kann.“

Verschlüsselung wird inzwischen von allen Anbietern und Dienstleistern in die Tat umgesetzt – und sogar weiterentwickelt. „Mit CAS PIA bieten wir beispielsweise KMUs und Selbstständigen eine reinrassige CRM-Lösung in der Cloud an, welche die Dokumente bereits beim Hochladen in die Cloud verschlüsselt“, berichtet Martin Hubschneider. „Künftig bieten wir für unsere Cloud-basierten Produkte neuartige Verschlüsselungskonzepte an, um die Daten nicht nur im Rechenzentrum,

sondern bereits auf dem Weg dorthin – also beim Bearbeiten von unterwegs – zu schützen."

Im Rahmen des Förderprojektes „MimoSecco" entwickelte CAS Software eine verteilte Speicherung in der Cloud mit. Das Prinzip: An drei Orten werden jeweils 2/3 der Daten verschlüsselt abgelegt. Sie werden von zwei autonomen Rechenzentren zurückgelesen und auf dem Endgerät vollständig zusammengefügt. Damit werde verhindert, dass Hacker Kundendaten in den Rechenzentren abgreifen.

„Selbst ein sehr konsistenter Einsatz von Sicherheitstechnologien wäre jedoch wirkungslos, wenn das Sicherheitsrisiko Mensch nicht genügend beachtet wird", gibt Lars Landwehrkamp, Sprecher von All for One Steeb zu bedenken. Daher würden stets auch die eigenen Mitarbeiter eingehend befragt. „Zudem unterziehen wir unsere Organisation freiwillig einer halbjährigen Überprüfung unserer Zertifizierung nach ISAE 3402. Hier geht es vor allem um die Prozesse, also die Anwendung unserer umfangreichen Sicherheitstechnologie im Tagesgeschäft."

Dass auch die regelmäßige Befragung keine Garantie darstellt, weiß Sergei Schlotthauer, Geschäftsführer des Herstellers EgoSecure: „Meist scheitert Datenschutz nicht an der technischen Umsetzung, sondern an der konsequenten Umsetzung." Er führt das Beispiel der „eigentlich sicheren Container-Verschlüsselungen" an, wie sie etwa die Software „Truecrypt" bietet. „Bequemlichkeit und der zusätzliche Zeitaufwand, etwa für das Öffnen und Schließen der Container, hindern Mitarbeiter, solche Lösungen einzusetzen", beklagt er. „Nur anwenderfreundliche Konzepte, die sich im Hintergrund um die Sicherheit kümmern, funktionieren auch langfristig." Im Idealfall werde jedem Benutzer einmalig eine Verschlüsselung zugewiesen. Damit könne dieser alle Daten öffnen, für die er eine Freigabe besitze.

MICHAEL MATZER