



IM INTERVIEW

Roland Peichl (re.),
Marketing-Leiter bei
Graupner, und IT-Leiter
Martin Schmelzer

Seite 20

MODELLBAUSPEZIALIST GRAUPNER

Ein eigenes IT-Modell

BRANCHE AUTOMOTIVE

Für Automobilzulieferer ist
Flexibilität höchster Trumpf

Seite 26

ERP-SOFTWARE

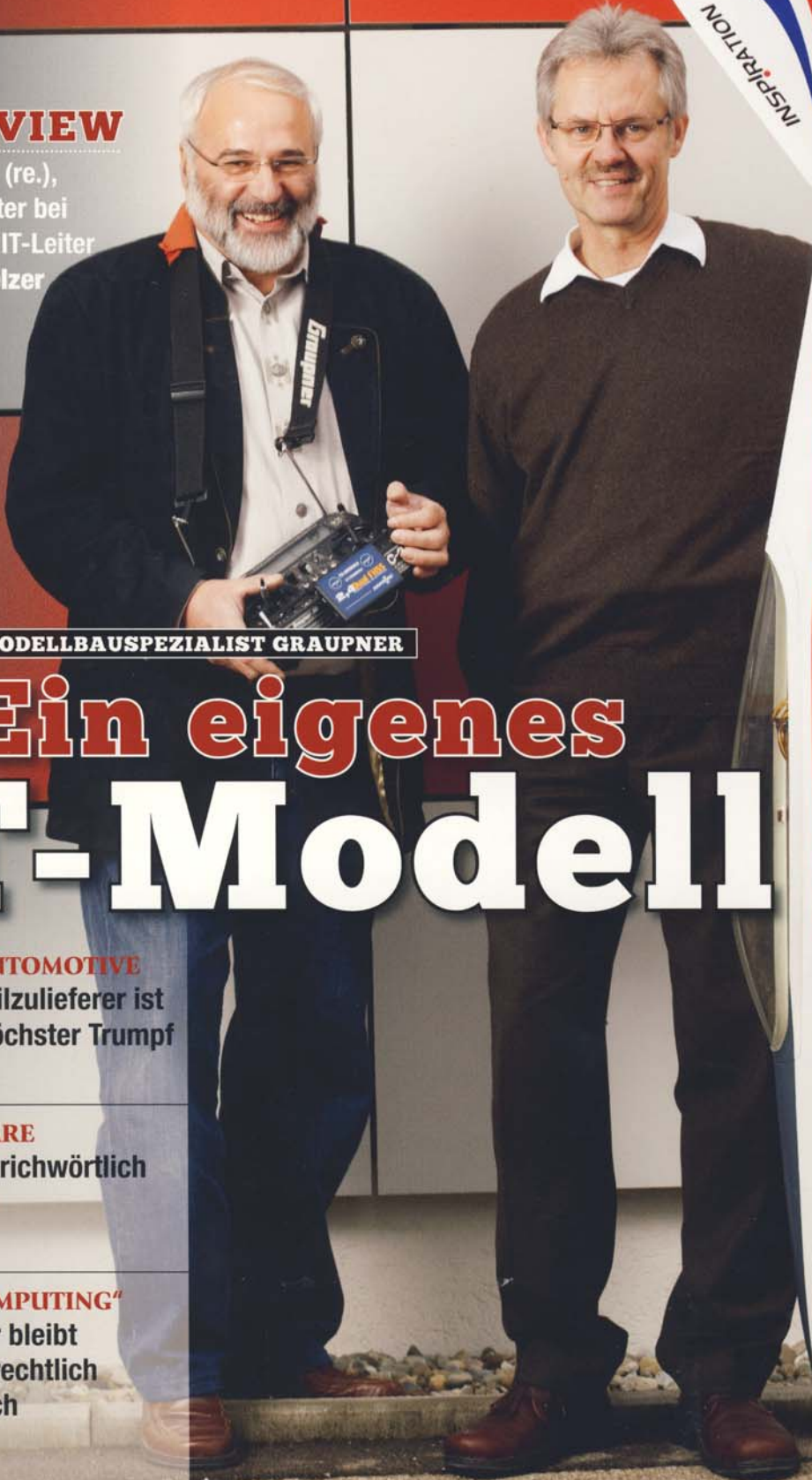
Alte Zöpfe sprichwörtlich
abschneiden

Seite 36

„CLOUD COMPUTING“

Auftraggeber bleibt
datenschutzrechtlich
verantwortlich

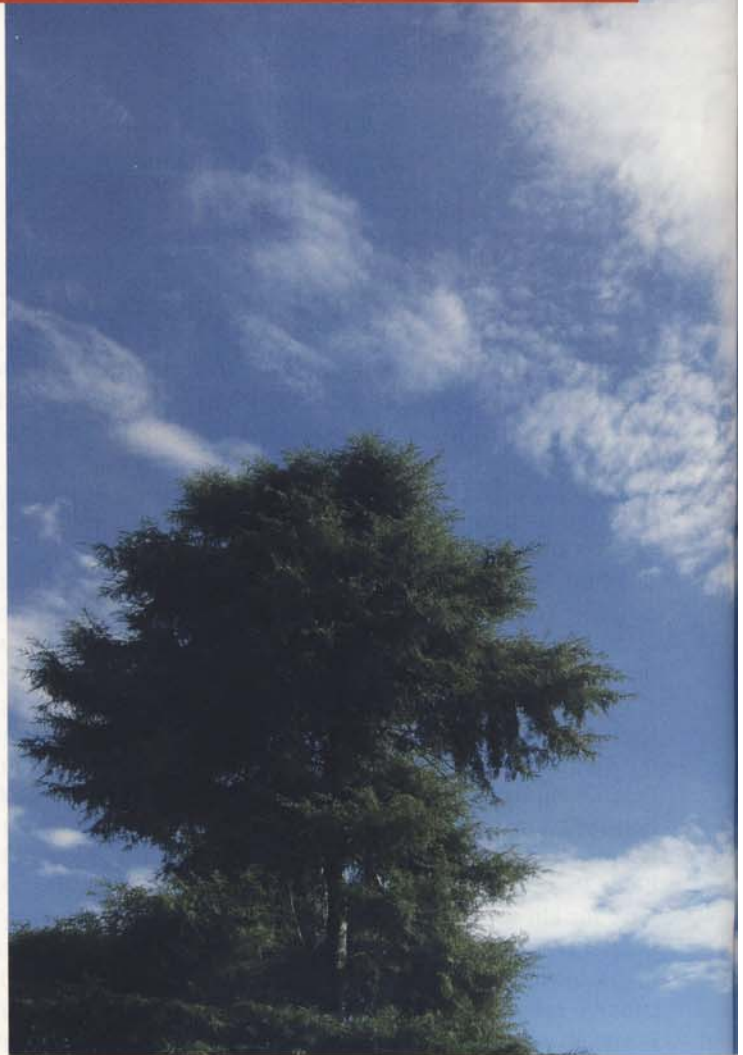
Seite 48



Definitionen von „**Cloud Computing**“ gibt es zuhauf. Dabei tragen die Angebote verschiedenster Hersteller wenig dazu bei, den Begriff zu erhellen. So gibt es derzeit am Markt Lösungen für **Software as a Service** (SaaS), **Infrastructure as a Service** (IaaS) oder **Platform as a Service** (PaaS). Doch was ist was?

WAS IST WAS?

Um Licht in das Dunkel zu bringen, hat sich beispielsweise das Beratungshaus Experton Group an einer Begriffserklärung versucht, die sich an die Definition des Modells der US-amerikanischen Bundesregierung anlehnt. Demzufolge ist Cloud Computing ein auf Nutzungsbasis abgerechnetes Modell für den On-Demand-Netzwerkzugriff auf einen gemeinsam genutzten Pool von konfigurierbaren Computing-Ressourcen (z.B. Netzwerke, Server, Storage, Applikationen, Services). Die fünf Hauptmerkmale von „Cloud Computing“ seien daher: On-Demand-Service, pervasiver Netzwerkzugang, standortunabhängige Ressourcen-Pools, schnelle Ausdehnung so-



Wer kennt Cloud Computing?

Kennen Sie eine gängige Definition für Cloud Computing?

Ja

28%

Nein

72%

Wäre der Bezug von Software aus der Wolke eine Alternative für Ihr Unternehmen?

Ja

25%

Nein

68%

Dazu müssten die Anbieter ihre Angebote konkretisieren

7%

Hegen Sie gegenüber der Nutzung von Cloud Computing-Lösungen rechtliche Bedenken?

Ja

17%

Nein, obwohl mir rechtliche Bedenken bekannt sind

12%

Nein, rechtliche Bedenken sind mir auch nicht bekannt

19%

Ich weiß nicht, was Cloud-Computing-Lösungen sind

52%

Quelle: Techconsult für IT-MITTELSTAND



wie eine nutzungsabhängige Bezahlung. Im Rahmen der drei Cloud-Bezugsmodelle SaaS, PaaS und IaaS (siehe Kasten unten) gibt es laut Experton vier verschiedene Einsatzszenarien, die jeweils intern oder extern betrieben werden können:

- **Private Cloud:** wird von einem einzigen Unternehmen gekauft bzw. gemietet und ausschließlich für diese Organisation betrieben.
- **Community Cloud:** wird von mehreren Organisationen mit denselben Anforderungen gemeinsam genutzt.
- **Public Cloud:** gehört einer Organisation, die standardisierte Cloud Services an die breite Öffentlichkeit und/oder Unternehmen verkauft.
- **Hybrid Cloud:** eine Mischung aus zwei oder mehreren Clouds, die zum Zweck der Daten- bzw. Applikationsportabilität miteinander verbunden werden.

Soviel zur Theorie. In der Praxis zeigt sich, dass vor allem mittelständische Unternehmen dem Cloud Computing alles andere als zugeneigt sind. So brachte eine Erhebung der Marktanalysten von Techconsult (siehe Umfrage S. 48) zutage, dass 72 Prozent der befragten Mittelständler überhaupt nicht wissen, was sich hinter dem Begriff versteckt. Selbstredend kommt daher der Bezug einer Cloud-Lösung als Alternative zu herkömmlichen Modellen für 68 Prozent

Delivery-Modelle des Cloud Computing

Software as a Service (SaaS) ist ein Modell für den On-Demand-Einsatz von Applikationen; dabei lizenziert der Anbieter seine Software und potentiell auch die von Drittanbietern für die Nutzung über das Internet.

Platform as a Service (PaaS) ist ein web-basiertes On-Demand-Modell für eine skalierbare, gemeinsam genutzte Umgebung von Lösungslayern und der zugrunde liegenden Infrastruktur für die schnelle Entwicklung und den Einsatz von Applikationen.

Infrastructure as a Service (IaaS) ist ein internetbasiertes On-Demand-Modell für eine gemeinsam genutzte, virtuelle Infrastruktur, die für alle möglichen Einsatzzwecke dynamisch bereitgestellt werden kann.

Quelle: Experton Group



„Üblich ist zumindest ein monatlicher Report des Cloud-Anbieters, der die Verfügbarkeit der Rechenzentren und des Netzwerks dokumentiert“, so **Patrick Pulvermüller**, Geschäftsführer bei Host Europe.



Enikő Vivien Visky, Regional Director bei Balabit: „Auch in einer Cloud haben Administratoren die Möglichkeit, Kundendaten unbemerkt zu kopieren oder zu manipulieren.“



Dr. Wolfgang Kraemer, Vorstandsvorsitzender der imc AG: „Der Dienstleister darf die ihm überlassenen Daten nicht länger aufbewahren, als gesetzliche Vorschriften oder vertragliche Verpflichtungen dies erfordern.“

der Unternehmen nicht infrage. Und sieben Prozent würden einen Einsatz von Cloud Computing erst in Erwägung ziehen, wenn die Anbieter ihre Angebote konkretisiert hätten.

Eine Untersuchung des Beratungshauses A.T. Kearney kam im August 2009 zu ähnlichen Ergebnissen. Nur bei zehn Prozent der an der Studie teilnehmenden Unternehmen aus Deutschland, Österreich und der Schweiz sei „Cloud Computing“ bislang ein fester Bestandteil der IT-Strategie. Als wesentliche Gründe für den zögerlichen Umgang mit Cloud Computing nannten die IT-Manager Sicherheitsbedenken, Kontrollverlust und fehlende Angebotstransparenz.

Die Verantwortung bleibt

Gedanken um ihre Sicherheit können sich mittelständische Unternehmen nie genug machen, gerade wenn es um so sensible Themen wie den Datenschutz geht. Bei der Anwendung von Cloud Computing könnte es mit dessen Einhaltung schnell kritisch werden, wie von IT-MITTELSTAND befragte Experten erklären.

Laut Bundesdatenschutzgesetz (BDSG) ist der Auftraggeber für die Einhaltung der Datenschutzregeln verantwortlich, auch wenn ein Dritter die Daten für ihn speichert (§ 11 Abs. 1 BDSG, siehe Rechtsbeitrag S. 62). „Wichtig ist, dass trotz der Nutzung einer Cloud die Verantwortung für die Daten und die datenschutzrechtliche Compliance beim Anwenderunternehmen verbleiben“, betont Thomas Jansen, Partner der Wirtschaftskanzlei DLA Piper in München. Daher gilt es, die technischen und organisatorischen Maßnahmen des Serviceanbieters für den Schutz der Daten sorgfältig zu prüfen.

Hinsichtlich der technischen Sicherheit empfiehlt Christoph Föckeler, Director Sales Consulting bei Salesforce.com, darauf zu achten, dass der Anbieter nach ISO 27001 und SAS/70, Type II zertifiziert ist. Beide Regelwerke stellen hinsichtlich Hochverfügbarkeit und Backup höchste Ansprüche und seien damit ein wichtiges Merkmal für den Kunden. Außerdem sollten die Anwenderunternehmen ihre bisherigen Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit an ihren Cloud-Betreiber weitergeben, um eine



KURZINTERVIEW

Schnell loslegen

➔ **Die knapp 30 Mitarbeiter** starke Amiando AG bietet eine webbasierte Applikation zur Organisation von Veranstaltungen im Geschäfts- wie im Freizeitbereich. Rund 25.000 Veranstalter organisieren kommerzielle oder private Events über den Webservice der Münchener. IT-MITTELSTAND sprach mit dem Finanzchef und Mitbegründer von Amiando, Sebastian Bärhold, über den Einsatz einer cloud-basierten Customer-Relationship-Management-Lösung (CRM) im Unternehmen.

ITM: Warum haben Sie sich für eine Cloud-Lösung und nicht etwa für den Eigenbetrieb der Software entschieden?

Sebastian Bärhold: Im Kundenbeziehungsmanagement haben wir in der Vergangenheit verschiedene Lösungen eingesetzt, von der Kontaktpflege und Kundenverwaltung in Excel, über eine eigens entwickelte Anwendung bis hin zum Einsatz eines Open-Source-CRM-Systems. Zufrieden waren wir damit allerdings nie: Alle Lösungen waren in der Handhabung zu sperrig, keine konnte wirklich an unsere Geschäftsanforderungen angepasst werden. Zudem waren weder eine strukturierte Datenbearbeitung noch ein Gesamtüberblick über alle Daten möglich.

Wichtig war uns, dass wir mit der Cloud-Computing-Lösung von Salesforce.com sofort arbeiten konnten. Zudem lässt sich die webbasierte Anwendung problemlos skalieren und anpassen. Und es besteht die Möglichkeit, über Web-APIs Drittsysteme einfach anzubinden.

ITM: Wie nutzen Sie die Lösung?

Bärhold: Wir sehen in der Sales Cloud beispielsweise, wenn sich unsere Nutzer auf unserer Plattform anmelden. Direkt aus dem CRM-System heraus können wir ihnen einen maßgeschneiderten Service anbieten. Ein Teil unserer Kundenansprache erfolgt automatisiert über Vorlagen. Die Implementierung dieser Funktionalität war in rund einem Monat abgeschlossen.



Sebastian Bärhold, Finanzchef und Mitbegründer von Amiando

ITM: Wer garantiert Ihnen die Rechtssicherheit für die ausgelagerten Daten?

Bärhold: Ein guter Cloud-Computing-Anbieter bietet seinen Kunden schon aus Eigeninteresse höchste Sicherheit. Auf unseren Cloud-Anbieter setzen unter anderem auch Finanzdienstleister, was die Lösungen aus unserer Sicht sehr vertrauenswürdig macht. Zudem wissen wir beispielsweise, dass die Rechenzentren des Anbieters regelmäßig von zertifizierten Sicherheitsanbietern überprüft werden und dem ISO 27001-Standard oder den internationalen Vorschriften nach SAS/70, Type II entsprechen. Wir selbst würden uns einen solchen Sicherheitsstandard vermutlich nicht leisten. ➔ |S

lückenlose Nachweiskette aufrechtzuerhalten. „Denn auch in einer Cloud verwalten Administratoren mit Superuser-Rechten Server und Datenbanken – und haben die Möglichkeit, Kundendaten unbemerkt zu kopieren oder zu manipulieren“, gibt Enikö Vivien Visky, Regional Director bei dem Sicherheitsanbieter Balabit zu bedenken. Die Anforderungen an den Umgang mit personenbezogenen

Daten ergeben sich aus §§ 9 und 11 und der Anlage zu § 9 BDSG. „Diese Anforderungen gelten auch für Cloud-Computing-Anwendungen. Anbieter einer Cloud haben technisch wie organisatorisch eine Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sicherzustellen“, so Dr. Thomas Jansen. Jedes Anwenderunternehmen sollte sehr genau prüfen, ob

der in Betracht gezogene Service Provider die Erfüllung dieser Anforderungen vertraglich zusichert. „Wenn nicht, Finger weg“, bringt es Dr. Jansen auf den Punkt.

Des Weiteren besagt § 11 des Bundesdatenschutzgesetzes, dass eine privilegierte Auftragsdatenverarbeitung nur dann vorliegt, wenn die Verarbeitung im Inland, innerhalb der EU oder innerhalb eines Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum stattfindet. „Vertraglich sollte daher vereinbart werden, dass der Auftragsdatenverarbeiter nicht berechtigt ist, die Daten ins EU-Ausland zu übermitteln oder dort zu verarbeiten. Eine Unterbeauftragung ist grundsätzlich nur mit Zustimmung des Auftraggebers zulässig“, erklärt Dr. Thomas Jansen. Da bei einer Übermittlung personenbezogener Daten in Nicht-EU-Länder ein Tatbestand vorliegt, der einer besonderen Rechtfertigung bedarf, müssen bestimmte Maßnahmen getroffen werden. Durch die Vereinbarung von sogenannten „Binding Corporate Rules“ könne laut Dr. Jansen auch außerhalb der EU ein hinreichendes Datenschutzniveau sichergestellt werden. Und Carsten Jording, Director Application Hosting bei der Nionex GmbH, ergänzt: „Unternehmen sollten nur einen Cloud-Anbieter auswählen, der von vorne herein garantiert, dass die Daten in einem oder in mehreren definierten Rechenzentren verbleiben und nicht automatisch in ein Rechenzentrum transferiert und abgelegt werden, das sich in einem unerwünschten Land befindet.“

Einen weiteren Tipp, um herauszufinden, wo die eigenen Daten liegen, gibt Patrick Pulvermüller, Geschäftsführer bei Host Europe in Köln: „Technisch kann man den Standort der Daten zumindest annähernd auch über Traceroutes herausfinden.“ Dabei handelt es sich um ein Diagnosewerkzeug, mit dem ermittelt werden kann, über welche IP-Router Datenpakete bis zum Ziel-Host übertragen werden. „Damit kann man erkennen, dass beispielsweise www.itmittelstand.de bei dem Hosting-Provi Hetzner im RZ10 liegt. Eine Anfrage bei Hetzner würde uns nun verraten, wo das RZ10 ist“, so Pulvermüller.

Wichtig sind zudem feste Regelungen darüber, was nach Vertragsende mit den vorgehaltenen Unternehmensdaten passieren soll. „Der Dienstleister darf die ihm überlassenen Informationen, ein-



„Trotz Cloud-Nutzung liegt die Verantwortung für die Daten und die datenschutzrechtliche Compliance beim Anwenderunternehmen“, betont **Thomas Jansen**, Partner der Wirtschaftskanzlei DLA Piper.



Laut **Christoph Föckeler**, Director Sales Consulting bei Salesforce.com, sollte ein Cloud-Anbieter nach ISO 27001 und SAS/70, Type II zertifiziert sein.

schließlich der Daten, nicht länger aufbewahren, als gesetzliche Vorschriften oder vertragliche Verpflichtungen dies erfordern“, betont Dr. Wolfgang Kraemer, Vorstandsvorsitzender des E-Learning-Spezialisten imc AG in Saarbrücken. Nach Beendigung der Zusammenarbeit habe der Anbieter unverzüglich die im Zusammenhang mit der Aufgabenerfüllung gespeicherten personenbezogenen Daten, einschließlich aller hiervon gefertigten Kopien, an den Anwender zurückzuspielen. Auch müsse er diese bei sich selbst nicht reproduzierbar löschen, soweit nicht eine gesetzliche Aufbewahrungspflicht besteht. „Hierbei wäre die Löschung unverzüglich nach Ablauf der Aufbewahrungsfrist vorzunehmen“, so Dr. Wolfgang Kraemer, „und dem Anwender unverzüglich eine

schriftliche Bestätigung zu erteilen, aus der sich gegebenenfalls auch der Umfang des etwaigen noch aufzubewahrenden Datenbestandes ergibt.“

Drum prüfe, wer sich lange bindet

Doch nicht nur seitens des Anwenders gilt es, Vorsorge zu treffen und sich vertraglich bestmöglich abzusichern. So müssen die Cloud-Anbieter selbst Maßnahmen ergreifen, um den Zutritt zur Cloud-Infrastruktur und den Zugriff auf die Daten ihrer Kunden zu kontrollieren. Je nach bereitgestellter Applikation kommen weitere Maßnahmen hinzu, die zum Beispiel ausweisen, welche Änderungen an den personenbezogenen Daten durch welchen Nutzer vorgenommen werden und wie sicher die personenbezogenen Daten an Fremdsysteme übergeben werden. „Letztendlich sind all die Maßnahmen zu ergreifen, die auch bei einem klassischen Hosting erforderlich sind“, fordert Carsten Jording von Nionex. Die .com-Cloud-Anbieter würden jedoch, außer der Behauptung „die Daten sind bei uns sicher“, in diesem Punkt leider recht wenig liefern.

Im Rahmen der Vertragsvereinbarungen sollten die Anbieter von Cloud-Services ihren Kunden zudem regelmäßige Prüfberichte zukommen lassen. „Branchenüblich ist zumindest ein monatlicher Report, der die Verfügbarkeit der Rechenzentren und des Netzwerks dokumentiert“, berichtet Patrick Pulvermüller. Für Christoph Föckeler von Salesforce.com wäre ein Bericht pro Monat indes viel zu wenig: „Die Unternehmen sollten darauf Wert legen, dass ihr Anbieter Informationen über Zertifizierungen, Verfügbarkeit, Performance und Sicherheit in Echtzeit online zur Verfügung stellt.“

Generell sollte der Prüfbericht eine Auflistung von Störungen, die zu Serviceeinschränkungen oder -ausfällen geführt haben, genauso beinhalten wie die Reaktionszeiten des technischen Supports und die Wiederherstellungszeiten nach einer Störung. Laut Patrick Pulvermüller schließen sich an einen solchen Report idealerweise Handlungsempfehlungen seitens des Service Providers an, beispielsweise wenn Systeme wiederholt durch Überlastung ausfallen und ein zusätzlicher Arbeitsspeicher oder Server das Problem beheben würden. ➔ **Ina Schlücker**