Verlagsbeilage, März 2012

‹kes›
Die Zeitschrift für Informations-Sicherheit

special

IT·Grundschutz Informationsdienst

WIK Zeitschrift für die Sicherheit der Wirtschaft

Sicheres Cloud-Computing

SecuMedia

CeBIT 2012: „Managing Trust“ ab S.18

Die technische Basis von Cloud-Computing sind standardisierte, modulare, adaptive Rechenzentren. Ihr großer Vorteil liegt darin, dass sie sich schnell an veränderte Erfordernisse anpassen lassen.

Ein sicheres RZ ist die Basis für sicheres Cloud-Computing

Auf festem Grund

Es gibt diverse Systeme, die die Sicherheit von Rechenzentren und damit sichere Lösungen für das Cloud-Computing gewährleisten. Welche das sind, beschreibt unser Beitrag.

Von Bernd Hanstein, Rittal

Um eine Cloud-Computing-Plattform wirksam abzusichern, müssen alle Aspekte berücksichtigt werden, die die Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Informationen gefährden können. Im Vordergrund stehen hierbei ein gut strukturiertes Vorgehensmodell für alle IT-Prozesse, der Aufbau einer Sicherheitsarchitektur zum Schutz der Ressourcen und die Isolierung von Mandanten. Unabhängig davon, ob es sich um eine Public-Cloud oder Private-Cloud handelt, ist die robuste Trennung der Kunden-, Abteilungs- oder Nutzerdaten auf allen Ebenen des Cloud-Computing-Stacks (Anwendung, Server, Netze, Storage) eine grundlegende Anforderung an jede Cloud-Computing-Plattform.

Standardisiert, modular, adaptiv

Der Schutz von personenbezogenen Daten in jeder Cloud verlangt angemessene technische und organisatorische Maßnahmen. Hinzu kommen Compliance-Anforderungen des Kunden und gesetzliche Regelungen für spezifische Daten. Notwendige Maßnahmen müssen vor Nutzungsbeginn einer Cloud-Lösung definiert und umgesetzt werden.

Die technische Basis von Cloud-Computing sind standardisierte, modulare, adaptive Rechenzentren. Ihr großer Vorteil liegt darin, dass sie sich schnell an veränderte Erfordernisse anpassen lassen. Durch das flexible Bereitstellen von IT-Diensten und einer dynamischen Infrastruktur entstehen deutliche Kosteneinsparungen. Da Software-Applikationen auf virtualisierten Server-Farmen sehr schnell zu- oder abgeschaltet werden können, lassen sie sich genau entsprechend dem aktuellen Bedarf skalieren – bei gleichzeitig höchster Verfügbarkeit der Dienste.

Diese Flexibilität muss sich auch in der physischen Infrastruktur der Cloud- Rechenzentren widerspiegeln. Diese setzt sich vor allem aus der Stromversorgung und -absicherung sowie der Kühlkette zusammen. Hierzu sind zwei Basistechnologien notwendig: eine dynamisch adaptive Infrastruktur und eine intelligente Management-Software.

Die Betreiber der Rechenzentren müssen die Sicherheit

ihrer Anlagen nach dem aktuellen Stand der Technik gewährleisten. Insgesamt sollte ein Rechenzentrum einen Sicherheitsbereich bilden, der sowohl ausreichend vor Elementarschäden wie Gewitter, Brand oder Hochwasser als auch vor unbefugtem Eindringen schützt. Dies geschieht durch eine permanente Überwachung der Zugänge, beispielsweise durch Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und geschultes Sicherheitspersonal. Darüber hinaus sollte gerade bei der IT-Sicherheit darauf geachtet werden, dass zertifizierte Lösungen eingesetzt werden. Sie sorgen dafür, dass spätere Zertifizierungsprozesse des Rechenzentrums nicht unnötig in die Länge gezogen werden. Zudem verbessern sie die Ratings von Versicherungen und bei aktuellen Kreditvergaben. Insoweit sie schon kodifiziert sind, sollte man sich an die aktuellen europäischen IT-Sicherheitsstandards halten. Muss eine besonders hohe Verfügbarkeit gewährleistet sein, sollten die Daten in einem redundanten RZ vorgehalten werden, so dass der Ausfall eines ganzen Rechenzentrums kompensiert wird.

Sicherheitsvorkehrungen an den Bedarf anpassen

Allerdings sollten die Sicherheitsvorkehrungen auch nicht überdimensioniert werden. Nicht alle Bereiche des Rechenzentrums benötigen unbedingt die gleiche Sicherheitsstufe. Bei vielen Räumen (zum Beispiel technische Versorgungsräume) genügt ein Grundschutz. Die Server sollten allerdings auf der höchsten Sicherheitsstufe betrieben werden. Modulare Konzepte und Hochsicherheits-Serverzellen ermöglichen sinnvolle Abstufungen des Sicherheitsgrades. Somit können Kosten gesenkt werden, ohne das Sicherheitsniveau zu beeinträchtigen.

Ein wichtiger Aspekt bei einem Rechenzentrum ist eine flexibel skalierbare Infrastruktur, die mit den – manchmal sehr plötzlich – ansteigenden Anforderungen an die Rechenleistung mitwachsen kann. Dies beginnt schon bei den ausgewählten Server-Schranksystemen. Sie sollten ohne Komplikationen erweiterbar sein. Ein Beispiel für ein Server-Rack ist die TS 8-Plattform des Systemanbieters Rittal. Die Schränke können an allen Seiten nahtlos aneinander gereiht werden und haben sich aufgrund ihrer hohen Stabilität bei vergleichsweise geringem Gewicht zu einem weltweiten Systemstandard entwickelt.

Auf die richtige Temperatur kommt es an

Cloud-Computing-Lösungen setzen in der Regel sehr leistungsfähige Server voraus und benötigen daher auch eine entsprechende Kühlung. Bei den Racks sollte unbedingt darauf geachtet werden, dass sie gleichmäßig ausgelastet sind. Denn zu volle Serverschränke, aber auch solche mit großen „Löchern“, erschweren die optimale Kühlung. Zudem muss für jeden einzelnen Server der jeweilige Kühlbedarf ermittelt werden – am besten mittels einer thermischen Analyse, die klimatische Mängel schnell identifizieren und abstellen kann. Rittal bietet redundante Kühlsysteme, die bis zu 60 kW Kühlleistung in ein einzelnes Serverrack beziehungsweise in eine Gangschottung bringen. Da die Vermischung von Kalt- und Warmluft sehr verlustreich ist, sollten Kalt- oder Warmgänge eingerichtet werden. Darüber hinaus bieten Raumkühlungs-Systeme die Option einer direkten freien Kühlung über die kalte Außenluft. Dieses Verfahren ist besonders energieeffizient und kostensparend. Es kann bei Außentemperaturen bis 21 Grad Celsius eingesetzt werden. Damit die gesamte Infrastruktur skalierbar und redundant ist, müssen natürlich auch die Kühlsysteme modular aufgebaut sein.

Automatisierte Monitoring-Lösung

Um Störungen und Ausfällen vorzubeugen, ist eine regelmäßige Wartung der Rechenzentrums-Komponenten von großer Bedeutung. Daher vereinbaren IT-Abteilungen oftmals mit den Fachabteilungen strikte Service-Level-Agreements (SLA), um die Verfügbarkeit der Infrastruktur sicherzustellen. Fachabteilungen erwarten eine Verfügbarkeit von 99,9 Prozent, was knapp neun Stunden Ausfallzeit im Jahr entspricht. Solche Werte können nur erreicht werden, wenn Sensoren und Software-Tools die Serverfarmen und Applikationen überwachen, verwalten und steuern.

Rittal bietet mit der Computer Multi Control (CMC) III eine automatisierte Monitoring-Lösung, die eine hohe Verfügbarkeit und Ausfallsicherheit gewährleistet. Sie ist frei skalierbar, selbst wenn das Rechenzentrum durch die Einbindung ganzer Server-Farmen rapide wächst. Sensoren sammeln in den Server-Racks und im Rechenzentrum Daten zum Beispiel über Temperatur, Luftfeuchtigkeit und -geschwindigkeit. Ein integrierter Infrarotsensor ermittelt beispielsweise, ob die Schranktür offen oder geschlossen ist. Die gemessenen Daten werden in einer Einheit konsolidiert und ausgewertet. Im Anschluss stehen sie über ein Web-Interface zur Verfügung oder können über das Simple-Network-Management-Protocol (SNMP) in die DCIM-Software RiZone eingebunden werden. Diese arbeitet die Messdaten auf und stellt sie strukturiert zur Verfügung. Die konsequente Zusammenführung sämtlicher Informationen des Rechenzentrums ermöglicht eine zuverlässige Beurteilung des Verfügbarkeitszustands der IT. Sind Messdaten außerhalb des grünen Bereichs, informieren Alarmsysteme die Administratoren innerhalb kürzester Zeit. Gesteuert wird die CMC III einfach über ein Notebook und einen USB-Anschluss.

Unterbrechungsfreie Stromversorgung unerlässlich

Das deutsche Stromnetz gilt zwar als verlässlich, dennoch gibt es auch hierzulande immer wieder Ausfälle. Daher ist es besonders wichtig, eine Infrastruktur in einem Rechenzentrum mit einer unterbrechungsfreien Stromversorgung (USV) gegen Spannungsausfälle und Störungen zu schützen. Nur so kann eine hohe Verfügbarkeit gewährleistet und SLAs eingehalten werden. Welches USV-System am besten zu den jeweiligen RZ-Anforderungen passt, hängt von vielen Faktoren ab, die im Vorfeld evaluiert werden müssen. Der wichtigste Aspekt ist dabei die Risikobewertung. Denn wie sich eine Minute Ausfallzeit auswirkt, ist für jedes Unternehmen eine individuelle Messgröße. Price Waterhouse Coopers hat in einer Studie festgestellt, dass ein Systemabsturz bei 75 Prozent aller Befragten mindestens 12.000 Euro Zusatzkosten verursacht. Bei 15 Prozent der Unternehmen liegen die geschätzten Aufwände sogar bei einer Million Euro und mehr.

Ein USV-System stellt sicher, dass die großen Datenmengen von Cloud-Computing-Lösungen auch bei Stromausfällen oder Störungen im Stromnetz sicher sind. Um keine überdimensionierten Anlagen zu nutzen, sind USV-Anlagen mittlerweile modular aufgebaut, wie beispielsweise die Power Modular Concept (PMC)-Familie von Rittal. Sie deckt die Gesamtlast nicht durch zwei identische Anlagen ab, sondern die USV-Chassis werden so mit Leistungsmodulen bestückt, dass bei einem fehlerhaften Modul die anderen Einheiten die Gesamtlast tragen können (n+1 Redundanz). Weil alle Module untereinander Load-Sharing betreiben, ist jedes Modul zu jeder Zeit abgesichert, die USV optimal ausgelastet und hat zudem einen sehr hohen Wirkungsgrad. Dieser ist gerade in Zeiten von steigenden Energiekosten immer wichtiger. Denn bereits ein Prozent größerer Wirkungsgrad kann die Stromkosten pro Jahr um mehrere Zehntausend Euro senken. Bei USV-Systemen ohne ausgangsseitigen Transformator wie die Rittal PMC-Serie, liegt der Wirkungsgrad bei 95 Prozent. Im Gegensatz zu herkömmlichen Anlagen kann der Anwender mit der aktuell geforderten Menge an Modulen starten und bei Bedarf erweitern.

Fazit

Es gibt mittlerweile eine Reihe von Systemen, die die Sicherheit der Rechenzentren und damit sichere Lösungen für die Private-Cloud gewährleisten. Mit einer unterbrechungsfreien Stromversorgung, einer übersichtlichen Verwaltungssoftware, automatisierten Monitoring-Lösungen und den richtigen Klimatisierungssystemen sind Anwender auf der sicheren Seite. Allerdings birgt auch eine Public-Cloud nicht nur Risiken für die IT-Sicherheit, sie eröffnet gerade kleinen und mittelständischen Unternehmen eine Reihe von Chancen. Speziell durch zentrale IT-Ressourcen, standardisierte Prozesse gepaart mit dem Spezialwissen der Cloud-Anbieter und Skaleneffekte, kann ein höheres Sicherheitsniveau bei gleichen Kosten erreicht werden. Kein Wunder also, dass die Analysten von PAC voraussagen, dass bis 2020 insgesamt etwa 20 Prozent der IT-Ausgaben für die Bereitstellung von Private- und Public-Cloud-Services aufgewendet werden.

CeBIT

CeBIT 2012: „Managing Trust“

Vom 6. bis 10. März 2012 öffnet die CeBIT wieder ihre Pforten. Dieses Jahr steht die Messe unter dem Leitthema „Managing Trust“. Unser Beitrag gibt eine Vorschau auf die Cloud-Themen. ***Seite 18***

Management und Wissen

Auf festem Grund

Ein sicheres Rechenzentrum ist die Basis für sicheres Cloud-Computing. Es gibt diverse Systeme, die die Sicherheit von Rechenzentren und damit sichere Lösungen für das Cloud-Computing gewährleisten. Welche das sind, beschreibt unser Beitrag. ***Seite 20***

Management und Wissen

Die Sorge Ernst nehmen

Beim Cloud-Computing stehen den vielen Vorteilen die Sorge um Datenschutz und Datensicherheit gegenüber. Auf dem jungen Wachstumsmarkt werden Sicherheit und Qualität für Anbieter von Cloud-Services somit zum entscheidenden Erfolgsfaktor. ***Seite 5***

Der Cloud-Leitstand

Um eine risikobasierte Entscheidung für ein angemessenes Cloud-Computing-Modell zu treffen, benötigt das Management entsprechende Informationen. Diese können nur vorliegen, wenn eine Strategie für das Sicherheits-, Governance-, Risk- und Compliance-Management entwickelt und die Risiken analysiert wurden. ***Seite 24***

Mehr Sicherheit mit Desktops aus der Cloud

Cloud-Dienste, wie das Bereitstellen von Desktop-Umgebungen über einen externen Service-Provider, bieten eine Möglichkeit, mobilen Mitarbeitern Zugang zur gewohnten Desktop-Umgebung – und damit zu allen Daten – zu geben, ohne dass dabei Sicherheitsrisiken für das Unternehmen entstehen. ***Seite 10***

Mehr Gefahr durch mehr Akteure

Das Risiko lässt sich nicht auslagern, meint unser Autor und fordert, dass vor allem der Zugriff auf Daten, Anwendungen und Infrastrukturen geregelt werden muss. ***Seite 27***

Schutz aus der Cloud

Um das Rennen gegen Hacker und Datendiebe zu gewinnen, setzen neue Security-Lösungen auf zusätzliche Schutzmodule, die mit Cloud-Technik arbeiten. ***Seite 14***

Die Cloud versichern

Die Verteilung der Risiken bei der Nutzung von Cloud-Computing kann beträchtliche Konsequenzen für die Haftung von Unternehmen und Cloud-Provider haben. Aus diesem Grund sollte der Versicherungsschutz entsprechend dem Risiko eingekauft beziehungsweise angepasst werden. Unser Beitrag zeigt, was in einem Cloud-Vertrag stehen sollte. ***Seite 29***

Datenhoheit durch Verschlüsselung

Werden Unternehmensdaten in der Cloud gespeichert, muss sichergestellt werden, dass nur Zugriff erhält, wer dazu berechtigt ist. Was Verträge schwer regeln können, bietet eine einfache und bekannte Technik: Verschlüsselung. ***Seite 16***

News und Produkte

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI
IT-Recht
BSI-Forum

<kes> ist *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - **Die Zeitschrift für Informations-Sicherheit** zum Probelesen zu.

☐ **ja,** bitte schicken Sie mir das **<kes> Special** zum Thema „Cloud Computing" gratis zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Leser-Service
Postfach 12 34
55205 Ingelheim