Sichere Informationstechnologie

Was braucht die Cloud?

Bild: © Nmedia/Fotolia.com

Sie ist der Wegbereiter für die digitale Wirtschaft: die Cloud. Flexible IT-Services on demand können Flexibilität und Kosteneffizienz schaffen. Ganze Prozessketten basieren mittlerweile auf Cloud-Infrastrukturen und müssen ohne Unterbrechung funktionieren. Um bei der bevorstehenden Digitalisierung der Industrie in vorderster Reihe zu stehen, bieten sich Infrastruktur-Anbieter als zuverlässige Partner für die Industrie an.

Die Digitalisierung der Prozesse, die Kommunikation zwischen Maschinen und die prädiktive Analyse großer Datenmengen sind die Zukunft der deutschen Wirtschaft und vor allem der Produktion. In der Automotive-Branche ist der Wandel bereits deutlich spürbar – schnell und flexibel auf Kundenwünsche zu reagieren wird hier zur absoluten Notwendigkeit. Dazu braucht es eine intelligente IT-Fabrik, die auf digitalen Fertigungsprozessen basiert, etwa Anlagen, die im Verbund arbeiten und miteinander kommunizieren. So lassen sich Störungen vorhersehen und die Transportwege innerhalb der Produktion optimieren. Doch ohne Cloud-Computing ist eine Industrie 4.0 schwer denkbar. Bereits knapp 40 Prozent der Unternehmen im Automobilbereich haben daher die Migration in die Private Cloud bewältigt. Auch mittelständische Unternehmen haben die Zeichen erkannt und steigen nach und nach auf den Zug in Richtung digitale Wirtschaft auf. Die Ziele sind klar: Prozesse verschlanken und mehr Flexibilität gewinnen.

Kostenaspekt entscheidend

Aber auch der Kostenaspekt spielt eine entscheidende Rolle: Ohne skalierbare Cloud-Services ist die wirtschaftliche Nutzung von High-Performance-Technologien beispielsweise im Bereich Big Data kaum möglich. Als größte Hürden für die Umsetzung einer Industrie 4.0 geben Unternehmen laut IDC-Studie 'Industrie 4.0' aus dem Jahr 2014 neben der Finanzierung vor allem die Themen Datenschutz und Datensicherheit an. Besonders im Rahmen von Big Data-Analysen erhobene Informatio-

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 6/2015.

Digitales Belegexemplar mit freundlicher Genehmigung des Fachmagazins IT&Production. Dieses Dokument ist ausschließlich zur elektronischen Speicherung durch den Autor sowie zur Weitergabe per E-Mail bestimmt. Abweichende Verwendung nur mit Zustimmung des Verlages.

nen gilt es vor unerlaubten Zugriffen zu schützen. Bezieht ein Unternehmen Infrastruktur und Services aus der Cloud, liegt diese Aufgabe beim Provider. Er muss das Rechenzentrum umfassend absichern – von der Zugangskontrolle über die Datenverschlüsselung bis hin zum Einsatz von Intrusion Prevention-Systemen, die mögliche Angriffe aufdecken und abwehren. Auch die Datenübertragung muss geschützt werden, etwa über ein sicheres VPN-Netzwerk. Weitere Sicherheitsmechanismen müssen beim Provider und dem Unternehmen greifen. Dazu zählt das Identity and Access Management (IAM). Dieses umfasst Rechte- und Rollenbeschreibungen, die definieren, welche Mitarbeiter in welchem Umfang Zugriff auf die in der Cloud gespeicherten Daten und Anwendungen haben. Die Identifikation kann über Smart Cards, Einmalpasswörter, Stimmerkennungssoftware oder den Fingerabdruck erfolgen. Wichtig ist in jedem Fall, dass die Lösung höchstmögliche Sicherheit bei größtmöglicher Benutzerfreundlichkeit bietet.

Null Fehler sind das Maß

Neben Cyber-Angriffen ist in den Medien immer wieder die Rede von System- und Serverausfällen großer Unternehmen. Das zeigt einmal mehr, dass die Verfügbarkeit der IT-Services ein nicht zu unterschätzender Aspekt bei der Partnerwahl ist. Schon ein defekter Netzwerkstecker kann die gesamte Stromversorgung unterbrechen und den Betrieb einfrieren. Ein Szenario, das in einer Industrie 4.0 komplette Produktionsprozesse zum erliegen und sogar Lieferverzüge mit sich bringen kann. Stellt ein Chemie-Unternehmen beispielsweise Produkte mittels Fermentierung her, macht eine Unterbrechung das Produkt unbrauchbar – und führt dadurch zu Lieferschwierigkeiten, Materialverlusten sowie zusätzlichen Entsorgungskosten. So hat die Verfügbarkeit von Systemen und Daten unmittelbaren Einfluss auf den Geschäftserfolg. Um besonders die Risiken eines Single Point of Failure – sprich von Elementen die nur einmal im System vorkommen – zu minimieren, ist daher eine redundant ausgelegte IT-Infrastruktur notwendig, zum Beispiel in Form von TwinCore-Konzepten. Hier wird das Rechenzentrum gespiegelt, inklusive aller Systeme und Anwendungen sowie der darin gespeicherten Daten. Gibt es in einem der Zwillinge eine Störung, springt der zweite unterbrechungsfrei ein. In Kombination mit doppelt ausgelegten Übertragungswegen ermöglicht dieser Ansatz eine Hochverfügbarkeit von bis zu 99,999 Prozent, was einer Ausfallzeit von etwa fünf Minuten im Jahr gleichkommt.

Gesamtkonzept benötigt

Alle diese hochmodernen Sicherheitstechnologien sind elementar. Sie funktionieren aber nur optimal, wenn der Provider aus den einzelnen Maßnahmen ein wirksames Gesamtkonzept schmiedet, das alle Anforderungen des Unternehmens abdeckt. Dazu muss der Dienstleister nicht nur technisches Know-how bezüglich Cloud-Storage und IT-Sicherheit bündeln, sondern auch Kenntnisse etwa in den Bereichen Business Analytics, energieeffizienter Rechenzentrumsbetrieb, Datenrecht et cetera. Da IT und Business immer mehr verschmelzen, sollte der Dienstleister zudem branchenspezifische Erfahrung aufweisen und bereits mit Partnern aus der Industrie zusammengearbeitet haben.

Vertraglich gesichert

Anbieter für Cloud-Services gibt es mittlerweile viele. Transparenz und Orientierung bieten Zertifizierungen, die Auskunft über den Grad der IT-Sicherheit bei potenziellen Geschäftspartnern geben und dabei helfen, die vorliegenden Angebote zu vergleichen. Sie basieren auf internationalen Normen und schließen unterschiedliche Sicherheitsmaßnahmen zum Schutz der IT-Services ein. Die ISO 27001-Zertifizierung legt beispielsweise spezielle Vorgaben für die Informationssicherheit bei der Entwicklung, der Bereitstellung und dem Betrieb von ICT-Lösungen fest. Ob Firewall oder TwinCore-Rechenzentrum – um letztlich sichergehen zu können, dass der Provider hält, was er verspricht, sind klare Vereinbarungen notwendig. In den Service Level Agreements (SLA) können das einzuhaltende Qualitäts- und Sicherheitsniveau sowie die Verfügbarkeit und Leistungsfähigkeit der bereitgestellten Ressourcen, aber auch Leistungen im Falle einer Störung definiert und verschriftlicht werden. ■

Der Autor Dr. Ferri Abolhassan
ist Geschäftsführer bei der
T-Systems International GmbH.

www.t-systems.de