MIDRANGE
MAGAZIN

02
2017

ITP VERLAG

IT-Konzepte und Wissen für POWER-Systeme im Unternehmensnetzwerk

305819198E · ISSN 0946-2880 · B 30465 · AUSGABE 332 · € 13,– · CHF 25,–

Interview zu IT-Security: Manfred Lackner, PROFI AG

„Konzentration auf die wesentlichen Risiken“

Schwerpunkte

ERP-Mobilzugriff
Cloud-Sicherheit

Technik

JSON-Daten
Verschlüsselung

Manfred Lackner, Vorstandsvorsitzender PROFI AG,
im Interview auf Seite 18

Keine Chance für Hacker

Sicherung von Unternehmensdaten in der Cloud

Die Aufkündigung des Safe-Harbor-Abkommens zwischen der EU und den USA hat demonstriert, wie unterschiedlich hoch das Sicherheitsniveau für Daten in der Cloud gehandhabt wird. Zwar wurde inzwischen mit Privacy Shield ein Nachfolger gefunden, dennoch müssen Unternehmen die Gefahren für ihre Daten in der Cloud weiterhin genau beobachten. Nur mit dem richtigen Know-how sind die Daten auch wirklich sicher.

Gerade in Deutschland sind die Vorbehalte gegenüber cloudbasierten BI-Lösungen groß. Dieses Misstrauen ist insbesondere im Mittelstand weit verbreitet. Es wird befürchtet, dass sich Unberechtigte Zugang zu sensiblen ERP-Daten verschaffen und diese Informationen der Konkurrenz zuspielen. Daher bleibt vielen Software-Anbietern meist nichts anderes übrig, als neben einer cloudbasierten auch eine On-Premise-Version ihrer Lösungen anzubieten. „Das Thema Cloud ist in Deutschland teilweise noch mit einem negativen Image behaftet, obwohl viele Unternehmen durch Outsourcing bereits vor langer Zeit den ersten Schritt in die Cloud gemacht haben", weiß Nikolaj Schmitz, CIO der G.I.B mbH aus Siegen. So haben sie zumindest einen Teil ihrer ERP-Prozesse in die Datenwolke verlagert. Das gilt in erster Linie für größere Unternehmen, die auf die Dienstleistungen von Cloud-Service-Anbietern wie etwa Rechenzentren setzen.

Privat, öffentlich oder hybrid

Doch Datenwolke ist nicht gleich Datenwolke, wie bereits die Unterscheidung in Private, Public und Hybrid Cloud zeigt. In der Private Cloud erhält der Anwender spezifische ERP-Systeme, auf die nur er Zugriff hat. „Solange man von der Private Cloud spricht, besteht aber, abgesehen von den zusätzlichen Möglichkeiten der Provisionierung, kein großer Unterschied zum klassischen Outsourcing", sagt Schmitz. Dagegen verhält es sich bei der Public Cloud ganz anders. In der öffentlichen Datenwolke befinden sich standardisierte Anwendungen, auf die eine Vielzahl von Nutzern zugreifen kann. Ein Beispiel hierfür ist etwa die Reisekostenabrechnung, die alle Außendienst- oder Vertriebsmitarbeiter eines Unternehmens nutzen. Sie teilen sich also ein zentral zur Verfügung gestelltes System.

Was für die Reisekostenabrechnung in der Private Cloud noch funktioniert, scheitert bei komplexeren oder kundenspezifischen Anwendungen wie etwa im Supply Chain Management. So lassen sich beispielsweise Rückmeldungen eines Fertigungsauftrags, die für die Buchung von Wareneingängen benötigt werden, mit Standardanwendungen meistens nicht realisieren. Aus diesem Grund dienen Applikationen aus der öffentlichen Datenwolke häufig nur als Ergänzung zu bestehenden IT-Lösungen, denn dadurch kann man darauf verzichten, die entsprechende Anwendung ins On-Premise-System integrieren zu müssen. Die parallele Nutzung von On-Premise und Cloud wird als Hybrid Cloud bezeichnet.

Für welche Variante sich ein Unternehmen auch entscheidet, jede besitzt ihre eigenen Risiken, vor denen die sensiblen Firmendaten geschützt werden müssen. Innerhalb der EU werden spezifische Sicherheitsniveaus vorausgesetzt, die Cloud-Service-Anbieter erfüllen müssen. Mit dem Safe-Harbor-Abkommen haben die USA vertraglich zugesichert, diese Schutzstandards einzuhalten, wenn europäische Unternehmen Server nutzen, die in den Vereinigten Staaten stehen. Anders herum gesagt: Eigentlich würden US-Firmen keine so hohen Sicherheitsstandards gewährleisten, wie sie die EU vorschreibt. Mit Privacy Shield ist nun zwar ein Safe-Harbor-Abkommen getroffen, jedoch gilt dies nur zwischen der EU und den USA. In anderen Ländern gelten ganz andere, völlig unterschiedliche Sicherheitsstandards.

Experten raten daher dazu, auf deutsche Cloud-Service-Anbieter zu setzen oder zumindest solche zu wählen, die ihren Sitz in einem EU-Land haben. Allerdings ist das Unternehmen damit nicht von der Pflicht entbunden, die Sicherheitszertifizierungen des Anbieters genau zu überprüfen. Die von der EU festgelegten Sicherheitsstandards sind schließlich nicht das Nonplusultra. Der Anbieter oder das Rechenzentrum selbst muss zudem in

regelmäßigen Audits die eigenen Zertifizierungen von externen Stellen kontrollieren lassen.

Sicherheit für die Datenübertragung

Zur Cloud gehört nicht nur der Server, auf dem die Unternehmensdaten vorgehalten werden. Auch die Datenleitung kann von Hackern angegriffen werden. „Verschlüsselung bei der Datenübertragung ist daher das A und O", so IT-Leiter Schmitz. Eine robuste Verschlüsselung gewährleistet, dass auch bei der Datenübermittlung kein Unberechtigter Zugriff auf sensible Informationen erhält. Die Verschlüsselungstechnologien haben sich in den vergangenen Jahren stetig weiterentwickelt. So wird derzeit das bereits in die Jahre gekommene SSL-Protokoll durch TLS ersetzt. Mit TLS werden einige Sicherheitslücken des alten SSL-Protokolls endgültig geschlossen. Darüber hinaus kann TLS jedes höhere Protokoll, das auf TLS basiert, implementieren. Das ermöglicht Anwendungen und Systemen eine größere Unabhängigkeit.

Für die sichere Datenübertragung zwischen dem Unternehmen und einem externen IT-Dienstleister werden immer häufiger VPN-Tunnel eingesetzt. Die Forderung, dass die Daten während der Übermittlung Deutschland nicht verlassen sollen, um die Sicherheit während der Übertragung zu erhöhen, halten viele Experten jedoch für überzogen. „Dies widerspricht teilweise dem Grundgedanken des Internets", so Schmitz. Schließlich besteht dieser darin, die Welt miteinander zu verbinden und nicht, einzelne Staaten voneinander abzuschotten. In einer sich immer stärker vernetzenden Welt mit globalen Märkten dürfte diese Forderung ohnehin nicht zu halten sein.

Gerade Unternehmen, die Tochtergesellschaften im Ausland gründen oder dort andere Unternehmen aufkaufen, müssen ihre einzelnen Standorte untereinander vernetzen. Mitarbeiter benötigen für ihre alltägliche Arbeit einen schnellen und einfachen Zugriff auf interne Daten. Hierfür werden häufig Web-Anwendungen eingesetzt, durch die eine große Zahl an Nutzern ortsunabhängig über unterschiedliche Endgeräte auf ein und dieselbe Anwendung zugreifen können. „Ohne Web-Anwendungen kommen viele Unternehmen schon heute gar nicht mehr aus", weiß Schmitz. Web-Anwendungen finden ihren Einsatz zum Beispiel im Service und Support oder in der Anbindung von Lieferanten an ERP-Systeme. Wer für seine Web-Anwendungen eine sichere Verschlüsselung einsetzt, eine professionelle Firewall nutzt oder die Zugriffe auf die Anwendung über ein Monitoring Tool überwacht, minimiert das Risiko eines illegalen Zugriffs. Externe Dienstleister überprüfen zudem die getroffenen Sicherheitsmaßnahmen mit den Methoden der Hacker, um den Schutz der Daten zu gewährleisten.

Im Fall von Web-Anwendung existiert jedoch eine große Schwachstelle: Es sind die unterschiedlichen Endgeräte, die zum Einsatz kommen. „Aber auch in diesem Umfeld gibt es Lösungen, die ein zentrales und transparentes Management ermöglichen", erklärt Schmitz. Über solche Lösungen lassen sich etwa einheitliche Sicherheitseinstellungen für jedes im Einsatz befindliche Endgerät umsetzen. Natürlich können auch in diesem Bereich die erwähnten Sicherheitsmaßnahmen wie Verschlüsselung oder VPN-Tunnel eingesetzt werden. Darüber hinaus sollte die Anmeldung des Nutzers im Unternehmenssystem über ein mehrstufiges Authentifizierungsverfahren erfolgen.

Für seine Softwarelösungen Dispo-Cockpit Forecast und Dispo-Cockpit Vendor Managed Inventory nutzt G.I.B die Outsourcing-Dienstleistungen eines Partners, der nachweislich über das notwendige Know-how für IT-Sicherheitsmaßnahmen verfügt. So setzt G.I.B für den Zugriff auf interne Web-Anwendungen ausschließlich verschlüsselte Datenleitungen ein. Darüber hinaus minimieren Firewalls das Risiko eines erfolgreichen Hackerangriffs. Da sämtliche Zugriffe kontrolliert werden, kann auf einen Angriff schnell mit den adäquaten Gegenmaßnahmen reagiert werden.

Natürlich gilt auch in der IT, dass es keine 100-prozentige Sicherheit geben kann. Um seine Daten mit einem so hohen Sicherheitsniveau zu schützen, wie es bei G.I.B der Fall ist, muss einiges an Aufwand und Kosten in Kauf genommen werden. Wer jedoch an der Datensicherheit spart, spart am falschen Ende, denn der Diebstahl sensibler Informationen kommt jedes Unternehmen um ein Vielfaches teurer zu stehen. Nicht nur, dass damit Wettbewerbsnachteile verbunden sein können – vor allem das Vertrauen von Kunden und Geschäftspartnern ist verloren, wenn ein Unternehmen gemeinsam genutzte bzw. seine eigenen Daten nicht ausreichend gegen Missbrauch und Diebstahl schützt. **Marc Hankmann** ■

www.gib-dispo-cockpit.de