

Sicherheit in der Cloud

Der Begriff «Cloud» (frei übersetzt: Rechnen in der Wolke) ist zu einem richtigen Hype geworden. Praktisch jeder spricht darüber, alle Zeitschriften berichten darüber. Dieser Artikel geht nicht auf die Cloud ein, sondern soll einige Facetten der IT-Sicherheit zeigen, die es zu beachten gibt.

Gemäss einer aktuellen Studie der IDC ist die Erhöhung der IT-Sicherheit eines der grössten Ziele, um die Cloud zu nutzen. Aber genau dieser Punkt ist auch das grösste Hindernis, die eigene Infrastruktur in fremde Hände zu geben. Die Cloud wird für verschiedene Arten genutzt: Auslagerung von Rechenkapazität beziehungsweise Datenspeicher (IaaS), fertigen Programmpaketen (SaaS) und Programmierumgebungen (PaaS). Der Vorteil darin liegt in der einfach skalierbaren Lösung. Jedoch gilt es auch die Sicherheitsrisiken frühzeitig in die Planung einzubeziehen. Davon betroffen sind vor allem die Integrität und die Vertraulichkeit der Daten.

Je nach Anbieter der Cloud-Lösung werden die Administratoren-Rechte komplett dem Kun-

den übergeben. Andere ermöglichen ihren eigenen IT-Angebotern kompletten Zugriff auf die Kundendaten. Auch im ersten Fall muss sich der Anbieter um die Verteilung der Daten (Redundanz) beziehungsweise um die Sicherung dieser kümmern. Dazu benötigt er in der Regel ebenfalls Zugriff auf die Daten. Auf jeden Fall besteht die Gefahr, dass die Kontrolle über den Zugriff auf die eigenen Daten abgegeben wird. Somit ist nicht mehr klar, wer genau auf diese Daten zugreifen kann.

Generell kann natürlich davon ausgegangen werden, dass die Administratoren vertrauenswürdig sind. Doch welcher IT-Angestellte musste schon je seine Identität beweisen, zum Beispiel mit der Identitätskarte oder seine Vergangenheit offenlegen, zum Beispiel mittels Strafregisterauszug. Vermutlich die wenigsten. Verschiedene aktuelle Fälle zeigen, dass es immer wieder geschieht, dass sich jemand eine andere Identität aufbaut und so unbemerkt einen Datendiebstahl durchführen kann.

Eine vertragliche Lösung könnte eine Abhilfe sein (durch Definieren einer einzelnen oder

mehrerer Personen), doch dies widerspricht der Idee von Cloud Computing. Somit bleibt nur eine Verschlüsselung der Daten, um den Zugriff auf die eigenen Daten sicherzustellen. Bei einem Online Datenspeicher stellt dies in der Regel kein Problem dar, ja wird sogar von einigen Anbietern direkt in die zu nutzende Software integriert. Anders sieht es jedoch aus, wenn eine Applikation in der Cloud genutzt wird. Diese Applikation muss verständlicherweise auf die Daten zugreifen können und erwartet diese in unverschlüsselter Form.

Für einen Cloud-Anbieter macht die Lösung nur dann einen Sinn, wenn er die vorhandenen Ressourcen auf mehrere Kunden aufteilen kann. Dies stellt den nächsten «Knackpunkt» dar. Der Anbieter muss garantieren, dass die Daten sicher voneinander getrennt sind. In virtualisierten Um-

gebungen stellt dies, je nach Software, kein Problem dar. Die Virtualisierung von Kundendaten gehört hingegen nicht dazu (beziehungsweise es sind erst sehr wenige zertifizierte Lösungen auf dem Markt, die dies beherrschen und dadurch sehr teuer sind). Dies gilt auch für Datenbanken. Der Anbieter muss den Spagat zwischen sicherer Datenseparierung und den Kosteneinsparungen machen. Es empfiehlt sich genau abzuklären, wie der Anbieter mit dieser Problematik umgeht und welche Lösungen er umgesetzt hat.

Beachtet werden müssen auch länderspezifische Gesetze und rechtliche Anforderungen zu beachten. So verbietet es das Schweizerische Datenschutzgesetz, Daten ins Ausland zu transferieren, wenn keine Gesetzgebung zum Schutz dieser Daten besteht (DSB, Art 6, Abs 1). Die EU erfüllt diese Anforderung, Amerika gehört hingegen nicht dazu. Viele Cloud-Anbieter haben darauf reagiert und bieten ihre Cloud-Umgebungen in der EU an. Sollte jedoch ein Rechenzentrum ausfallen, werden die Daten an ei-

ZUM AUTOR

Dipl.-Ing, FH, CISSP, Andreas Wisler
IT-Redaktor Maschinenbau
Geschäftsführer GO OUT
Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.goout.ch
info@goout.ch



■ Anzeige



NOTZ METALL
part of the notz group

Notz Metall AG

Mit über 100 jähriger Erfahrung spezialisieren wir uns auf den Handel von:

- Bleche
- Dekorationsbleche
- Nahtlose und geschweisste Rohre
- Rohrzubehör
- Lebensmittel-, Pharma- und Aseptikarmaturen
- Handlaufzubehör
- Stabstahl
- Automatenstähle (anfasen, anspitzen)
- Bandstahl
- Draht & Profile
- Service-Center mit Anarbeitung nach Kundenspezifikation
- Eigenes Werkstofflabor zu Ihren Diensten

Notz Metall AG

CH - 2555 Brugg
Telefon +41 (0)32 366 77 55
Telefax +41 (0)32 366 77 34

Notz Metall AG

CH - 8603 Schwerzenbach
Telefon +41 (0)44 908 32 00
Telefax +41 (0)43 444 98 10

ISO 9001:2008
E-Mail: info@notzmetall.ch
Internet: www.notzmetall.ch

nen anderen Standort transferiert (oder sind bereits redundant dort abgelegt). So kann es schnell geschehen, dass die Datenschutzbestimmungen verletzt werden. Dieser Umstand sollte ebenfalls schriftlich festgehalten werden.

Oft wird unterschätzt, dass durch die Auslagerung eines Dienstes mehr Single Point of Failure entstehen, als gelöst werden. Zwischen dem eigenen Netzwerk und dem Anbieter entsteht ein grösseres Netzwerk mit weiteren Komponenten. Damit erhöht sich auch die Gefahr von Ausfällen. Klar kann dies wiederum durch Redundanzen gelöst werden (zum Beispiel durch eine redundante Internet-Anbindung zum Anbieter), doch auch dies widerspricht dem Cloud-Gedanken, da die Netzwerkpfade auf Seiten des Anbieters unbekannt sind. Oft sind auch verschiedene Provider zwischen dem eigenen Netzwerk und der Cloud. Daher sollte als dritter zu regelnder Punkt auch ein Nachweis über die Ausfallsicherheit des gesamten Netzwerkpades

definiert sein. Zusätzlich lohnt es sich, bereits im Vorfeld einen entsprechenden Notfallplan zu erarbeiten. Bevor die Wahl auf einen Anbieter fällt, sollten folgende Elemente beachtet werden:

- Verfügbarkeit der Cloud Security Lösung.
- Transparenz bezüglich der Lokation der Daten.
- Zertifizierung des Cloud Anbieters (SAS 70 Type II, ISO 27001).
- Unabhängigkeit gegenüber dem Anbieter.
- Umsetzung von Standards (ISO 20000, ITIL).

Die Cloud stellt alle beteiligten Parteien vor neue Herausforderungen, für welche es nur teilweise befriedigende Lösungen gibt. Daher sollten alle erwähnten Problemfelder für den eigenen Einsatzzweck gründlich überprüft und schriftlich festgehalten werden. Eine zusätzliche Risiko-Analyse hilft, die möglichen Schwachpunkte zu erkennen und im Vorfeld geeignete Massnahmen umzusetzen.

Automation beginnt schon an der Maschine.

Die ultrapräzisen Drehmaschinen für Feinst- und Hartzerspanung PD und SB sind mit Rundachsen, angetriebenen Werkzeugen und eigens entwickelten Spindeln ausgestattet. Die kreisform-, wiederhol- und messgenauen Maschinen für die Serienfertigung sind durch verschiedenste interne und externe Palettiersysteme und Roboter unkompliziert automatisierbar. Sie überzeugen mit Prozesssicherheit auch bei kleinsten Toleranzen.



SPINNER

Spinner AG
CNC-Präzisionsmaschinen
Weinlandstrasse 10
CH-8451 Kleinandelfingen

Tel. +41 52 301 21 55
Fax +41 52 301 21 54

info@spinner-ag.ch
www.spinner-ag.ch

Stand J21, Halle 1.1

PRODEX¹⁰

Drehen und Automation

SUPERBOLT®

Spitzentechnologie für Schraubenverbindungen

- sicher
- dauerfest
- lösbar

Swiss Perfection

- Entwicklung & Konstruktion
- Herstellung
- Installation

Mechanische Spannelemente



- für grosse Gewinde
- torsionsfrei
- ohne Spezialwerkzeug
- höchste Spannkraft
- einfach und schnell, auch beim Lösen
- ohne Setzungen
- höchste Sicherheit
- niedrige Kosten
- Standardprogramm: M20–M160
- Spezialausführungen bis M1000 und grösser



P&S Vorspannsysteme AG
CH-8735 St. Gallenkappel · Schweiz
T: +41 55 284 64 64 · F: +41 55 284 64 69
info@p-s.ch · www.p-s.ch