2.2 In sechs Schritten zu mehr Cloud-Security

Vor fünf Jahren hat sich noch kaum ein Unternehmen für die Sicherheit von Business-Software interessiert. Die Bedenken bezogen sich in der Regel auf Sicherheitslücken bei Daten, die Anwendungen selbst standen kaum im Fokus. Doch seit Unternehmen immer mehr Software in die Cloud verlagern, ändert sich diese Sichtweise zunehmend, denn die Cloud bietet neue Angriffsmöglichkeiten. Damit sind das Sicherheitsbewusstsein und auch die Anforderungen an das Know-how der Entwickler, die Anwendungen sicher machen sollen, sprunghaft gestiegen.

2.2.1 Mehr Risiken im Internet

Mit der zunehmenden Digitalisierung von Unternehmen und ganzen Wirtschaftszweigen nehmen die Risiken für Unternehmen durch das Internet zu, doch häufig mangelt es an der Umsetzung ganz grundlegender Sicherheitsmaßnahmen. Für Unternehmensdaten in der Public Cloud ist die Gefahr besonders hoch, und auch die zunehmende Verwendung mobiler Endgeräte im Zuge des Bring-Your-Own-Device-Trends (BYOD) bereitet IT-Managern vieler Unternehmen Kopfschmerzen.

Diese Smart Devices verfügen über ein komplett anderes Sicherheitsprofil als die klassischen Desktop-PCs. In der mobilen Infrastruktur steckt ein doppeltes Risikopotenzial: Die Geräte an sich genügen nur sehr niedrigen Sicherheitsstandards, und zusätzlich ist die nicht gesicherte Funkkommunikation ein beliebtes Angriffsziel. Neben den Daten kann auch die eigentliche Business-Software zur Gefahrenquelle werden. Mit dem Hosting in einer Public Cloud ergeben sich neue Angriffsszenarien. Durch die Auslagerung kritischer Geschäftsprozesse in die Cloud ist ein Unternehmen sämtlichen Gefahren ausgeliefert, die im Internet existieren, von Viren, Trojanern und Bot-Netzen bis hin zu Abhöraktionen und Spionage sowie plötzlichen Schließungen der Internetpräsenz. Im schlimmsten Fall steht eine ganze Firma still. Business-Software ist jedoch generell gar nicht dafür ausgelegt, sich vor solchen Risiken zu schützen. Viel wichtiger ist es deshalb für die Unternehmen, die Frage zu beantworten, wie beziehungsweise welche Daten und Anwendungen in die Cloud verlagert werden und wie sie dort an die Risiken anzupassen sind. Gehen Unternehmen die folgenden sechs Schritte, reduzieren sie das Risiko für Daten und Business-Software deutlich, ohne auf die Vorteile der Cloud verzichten zu müssen.

2.2.2 Auf Sicherheitszertifikate achten

Dem zunehmenden Bewusstsein der Kunden für die Sicherheit von Business-Software begegnen Softwareanbieter damit, dass sie ihre Produkte verstärkt auf Sicher-

heitslücken testen lassen. Anwender sollten deshalb auf Sicherheitsevaluierungen achten, wie sie zum Beispiel Spezialisten für Sicherheitstests – beispielsweise das Unternehmen Veracode – ausstellen, oder ihre Software durch Dritte prüfen lassen.

2.2.3 Business-Software unter die Lupe nehmen

Wenn Softwareanbieter trotz Zertifizierung Sicherheitsversprechen nicht halten, können sie haftbar gemacht werden. Ist der Anbieter aber nicht identifizierbar, wie etwa bei Open-Source-Komponenten, trägt der Anwender das Risiko, da er die Software eigenverantwortlich eingesetzt hat. Diese Problematik ist akut, da Business-Software-Architekturen nicht mehr von Grund auf neu und aus einem Guss geschrieben und aufgesetzt werden. Architekturen bestehen aus verschiedenen Komponenten, die von den unterschiedlichsten Anbietern entwickelt wurden beziehungsweise Open-Source-Module enthalten. Eine Bewertung dieser Gefahr lässt sich mithilfe öffentlicher Datenbanken bewerkstelligen, in denen die Risiken von Open-Source-Komponenten aufgelistet sind.

2.2.4 Daten nach Relevanz trennen

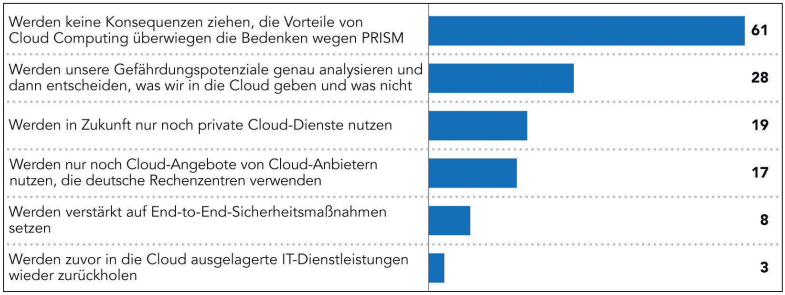
Grundsätzlich sollten sich Unternehmen Gedanken machen, welche Daten und Anwendungen sinnvollerweise in die Cloud ausgelagert werden können und welche besser on-premise im Unternehmen bleiben sollten. Handelt es sich um unkritische Informationen, steht einer Cloud-Verwendung nichts im Weg. Bei sensiblen und kritischen Daten erhebt sich jedoch die Frage, ob eine Schnittstelle in die Cloud angebracht ist. Dabei sind zwei Dinge generell zu beachten: Bei Business-Software aus der Public Cloud stellt der Anbieter in der Regel die Schnittstellen vorab ein, die der Anwender dann individuell konfigurieren sollte, damit nur die unkritischen Daten mit dem Internet verbunden sind. Darüber hinaus kann aber auch der Cloud-Betreiber in die Verantwortung genommen werden, denn grundsätzlich haftet er für die Sicherheit der Daten.

2.2.5 Verschlüsselung der kritischen Daten

Durch die in Service-Level-Agreements (SLAs) vertraglich geregelten Sicherheitsvorkehrungen kann ein Anbieter für Schäden durch Sicherheitslücken haftbar gemacht werden. Doch selbst wenn der Cloud-Betreiber höchste Sicherheit verspricht, bleibt immer ein Restrisiko. Zur Lösung dieses Problems bietet es sich an, die kritischen Unternehmensdaten zu verschlüsseln, bevor sie in die Public Cloud ausgelagert werden.

Eine Bearbeitung der Daten erst in der Public Cloud ist nicht möglich, weil das eine Entschlüsselung in der IT-Wolke voraussetzen würde, was die Verschlüsselung ad absurdum führen würde. Kritische Daten sollten deshalb nicht mit Busi-

ness-Software aus der Public Cloud bearbeitet werden. Gegenwärtig verschlüsselt nur ein Drittel der Unternehmen Daten, den Verzicht darauf begründen die anderen zwei Drittel auch mit erhöhtem Aufwand und verschlüsselungsbedingten Performance-Verlusten. In Zukunft wird zwar der Verschlüsselungsaufwand aufgrund höherer Rechenleistung geringer werden, es ist aber zu erwarten, dass dann auch die Gegenseite aufrüsten wird, was wiederum größere Sicherheitsschlüssel notwendig machen würde.



Konsequenzen aus den Abhörskandalen: Die meisten Unternehmen wollen auf die Vorteile des Cloud Computings nicht verzichten. Allerdings wird man Angebote und Provider künftig wohl genauer prüfen. Angaben in Prozent, Mehrfachnennungen möglich. (Quelle: Techconsult GmbH)

2.2.6 Mobile Geräte richtig sichern

Mit der zunehmenden Verwendung von Smart Devices im Unternehmensumfeld – besonders, wenn es um den BYOD-Trend geht – und der Entwicklung von Business-Software-Apps werden mobile Endgeräte ebenfalls zu einem Sicherheitsrisiko. Denn ob eine App auf das Internet zugreift und die Daten damit einem möglichen Angriff ausliefert, bestimmt die Vorkonfiguration, die der Anwender nicht beeinflussen kann. Deshalb wurden zum Schutz kritischer Daten Zusatzdienste entwickelt, die das Gerät in zwei „Sicherheitszonen" teilen und aus einem Smart Device virtuell zwei Geräte machen. Die private Zone ist nicht gesichert und quasi öffentlich zugänglich. Dort werden die Apps installiert. In der zweiten Zone, der Unternehmenszone, lassen sich dagegen keine Applikationen aufspielen. Dieser gesicherte Bereich hält ein „gehärtetes" Betriebssystem und die kritischen Daten vor.

Weil der Nutzer nur von der gesicherten Zone aus mit dem Unternehmen kommunizieren kann, sind die Kommunikationsprotokolle dort auch nur mit dem Unternehmen verbunden. Selbst wenn die Mitarbeiter ihre eigenen Geräte während der Arbeit nutzen, können Unternehmen diese Sicherheitsstrategie umsetzen, vorausgesetzt, sie entwickeln eine entsprechende Policy. In der Praxis werden solche Zusatzdienste bislang jedoch nur zögerlich eingesetzt, weil sie die Komplexität eines Geräts erhöhen.

2.2.7 Security-Response-Plan entwerfen

Trotz aller Sicherheitsmaßnahmen sollten sich Unternehmen auch auf den Ernstfall vorbereiten. Es muss ein Plan B, ein Security-Response-Plan, vorliegen, damit für den Notfall festgelegt ist, mit welchen Aktionen auf einen Angriff reagiert werden soll. Diese zweite Verteidigungslinie dient der Schadensbegrenzung, denn in solchen Situationen ist es maßgeblich, schnell und richtig zu reagieren. Bisher nutzen Unternehmen diese Möglichkeit allerdings noch zu selten.

2.2.8 Big Data = Big Risk?

Neben Cloud und Mobile Computing kommt mit Big Data eine weitere Gefahrenquelle auf Business-Software und Unternehmensdaten zu. Da unstrukturierte Daten für Business-Software bislang nur eine untergeordnete Rolle spielen, ist das Risiko zwar noch gering. Dennoch kann Big Data für das eigene Geschäft gefährlich werden, wenn immer mehr Systeme wie zum Beispiel auch Produktionsanlagen vernetzt werden. In Zukunft wird es immer wichtiger, riesige Berge an Business-Daten verarbeiten zu können. Schreckensszenarien wie die Sabotage von Fabriken über Cyber-Angriffe sind heute nur Thema von Science-Fiction-Filmen, könnten aber schon bald Realität werden.

Harald Schöning

Harald Schöning ist Head of Research der Software AG.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Acht Tipps für die sichere Cloud**
  (www.tecchannel.de/2040524)
- **Wie Open-Source-Software die Cloud antreibt**
  (www.tecchannel.de/2041280)
- **So schützen Sie sensible Daten in der Cloud**
  (www.tecchannel.de/2040289)
- **Private Cloud und Public Cloud sicher verbinden**
  (www.tecchannel.de/2040713)
- **Management-Tools für Cloud Storage**
  (www.tecchannel.de/2040495)
- **Cloud Security Services im Check**
  (www.tecchannel.de/2039927)
- **Cloud Computing für kleine und mittelständische Unternehmen**
  (www.tecchannel.de/2038994)