Database as a Service – ein Spielplatz für Hacker?

Martin Dombrowski, IMPERVA Inc.

Die steigenden Anforderungen an Qualität und Kosteneffizienz in Unternehmen sorgen dafür, dass Cloud-Dienste hier zunehmend an Bedeutung gewinnen. So wundert es kaum, dass auch Datenbanken mittlerweile als Cloud-Service angeboten werden.

Auf den ersten Blick haben Database-as-a-Service-Lösungen für Unternehmen ausschließlich Vorteile. Je nach Service Level Agreement muss der Anwender lediglich seinen Bedarf definieren – der Rest wird vom Service-Provider erledigt. Dazwischen gibt es selbstverständlich noch Abstufungen, inwieweit der Aufbau und die Pflege der Datenbank ausgelagert werden.

Bei virtuellen Lösungen auf diesem Gebiet lässt sich die Skalierung von Ressourcen schnell und problemlos bewerkstelligen. Aufgrund der Verteilung verschiedener Instanzen einer Datenbank auf unterschiedliche virtuelle Maschinen wird die Last bei Zugriffsspitzen durch viele Abfragen gleichzeitig sehr wirkungsvoll verteilt. Auch die Provisionierung neuer Datenbanken kann schnell durchgeführt werden und Erweiterungen sind zügig implementiert. Das spart Kosten und bietet Unternehmen höchstmögliche Flexibilität in Bezug auf Erweiterungen.

Dynamischer Anpassungsprozess

Der Betrieb von Datenbanken in virtuellen Umgebungen unterscheidet sich jedoch signifikant von dem konventioneller Lösungen. Es geht dabei nicht allein um eine Portierung einer bestehenden lokalen Lösung, sondern auch um einen dynamischen Anpassungsprozess. Die Kernaufgabe besteht in der Übertragung der vollen Funktionalität unter Beibehaltung der Integrität. Das ist ein recht kompliziertes Unterfangen, da bei der Virtualisierung einer Datenbank über mehrere physische Plattformen Zugriffe und Abfragen so geregelt sein müssen, dass es nicht zu mehrfachen Einträgen durch die gleichzeitige Nutzung verschiedener Instanzen der Datenbank kommt.

Ein Beispiel dazu ist eine Buchhaltungs-Datenbank, die eine Zahlungsanweisung

an einen Kunden erhält. Damit dieser Vorgang mit den entsprechenden Kunden- und Zahlungsdaten verknüpft wird, geht an die virtualisierte Datenbank eine entsprechende Anfrage heraus, die gleichzeitig an die unterschiedlichen Instanzen der Datenbank läuft. Nun ist es erforderlich, dass eine Sperre greift, die verhindert, dass der Vorgang mehrfach auf unterschiedlichen Instanzen durchgeführt wird.

Doch warum ist es notwendig, eine Datenbank in virtueller Umgebung auf unterschiedlichen Instanzen zu betreiben? Grund dafür ist die Auslastung der Server, die die Datenbank hosten. Auch die Zugriffe auf Datenbanken unterliegen nämlich Lastspitzen. Sie lassen sich zum Beispiel dadurch abfedern, dass sich redundante Systeme über mehrere virtuelle Maschinen erstrecken. Bei Auslastung eines Systems werden Anfragen weitergereicht und so ist es möglich, dass unterschiedliche Instanzen gleichzeitig agieren, was bei einer konventionellen Lösung leichter vermieden werden kann.

Herausforderung an die Sicherheit

Der Trend in Unternehmen zu „Database as a Service" (DBaaS) ist jedoch nicht nur in Bezug auf die technischen Besonderheiten eine Herausforderung, sondern stellt auch ein neues Sicherheitsrisiko dar. Das zeigt unter anderem ein Beispiel aus dem vergangenen Jahr, als ein Hackerangriff auf die kalifornische DBaaS-Plattform MongoHQ erfolgte, die von zahlreichen Cloud-Hosting-Diensten verwendet wird. Entdeckt wurden der Angriff und somit auch das Sicherheitsleck erst, nachdem ein Kunde gehackt worden war. Das Unternehmen reagierte daraufhin zwar professionell, entschuldigte sich bei dem Kunden, schilderte detailliert die entdeckten Sicherheitslücken und nannte konkrete Maßnahmen zu deren Schließung.

Das Beispiel zeigt allerdings, dass hier ein immenser Schaden hätte entstehen können. Möglich wurde die Attacke unter anderem deshalb, weil eine Support-Anwendung offen über das Netz und nicht ausschließlich über ein VPN nutzbar war. Zudem war keine Zwei-Faktor-Authentifizierung umgesetzt worden. Außerdem gab es kein klares User Rights Management. Es fehlten abgestufte Berechtigungen für das Service-Personal, sodass quasi jeder Mitarbeiter wie der Systemadministrator Zugriff auf sämtliche Kundendaten hatte.

Gefährdung für Unternehmen

Auch die aktuelle Studie „Assessing the Threat Landscape of DBaaS" *(siehe „www.imperva.com/download.asp?id=436")* belegt die Gefahr für die IT-Sicherheit durch Database as a Service. Die Separierung von Unternehmens-Intranet und Datenbank-Zugriff über einen externen Cloud-Service erleichtert es Angreifern ungemein, in das gleiche Netz wie die Cloud einzudringen. Wenn dieser Angreifer nämlich einen eigenen Dienst mit eigenem Account im Cloud Service anmeldet, kann er unter anderem Attacken auf die betreffende Datenbank direkt lancieren, ohne sich zuvor mühsam Zugang zu einem Firmennetz verschaffen zu müssen. Die Gefährdung für Unternehmen ist groß, da neben der Infektion durch Schadcode auch sensible Daten gestohlen werden können.

Für ihre Angriffe nutzen Kriminelle die Tatsache, dass ein interner Angriff auf Datenbank-Strukturen wesentlich einfacher durchgeführt werden kann als ein externer. Darüber hinaus belegt die Studie, wie einfach es für Anwender in einer Datenbank ist, sich höhere Zugriffsrechte zu verschaffen. Das vereinfacht sogenannte „Privilege-Escalation-Angriffe", bei denen entweder manuell oder sogar automatisiert tiefgreifende Aktionen in einer Datenbank durchgeführt werden können. Das kann im schlimmsten Fall zum Verlust des Datenbestands führen. Bereits heute ist aktuelle Schadsoftware in der Lage, sich mit Datenbanken zu verbinden, um dort gezielt Informationen zu manipulieren.

Von noch größerer Tragweite ist, dass Malware DBaaS sogar für ein Botnet-Management missbrauchen kann, wie das aktuelle Beispiel einer Shared-Hosting-Datenbank für „Command & Control" und Drop-Server zeigt. Dabei wird ein Schadcode injiziert, der sich selbst in weitere Datenbanken mit ähnlicher Struktur dupliziert und von dort weitere schädliche Aktivitäten ausführt. Diese Entwicklung macht es den Studienergebnissen zufolge wahrscheinlich, dass ein Angriff autonomer Malware auf interne Datenbanken von Unternehmen kurz bevorsteht.

Fazit

Unternehmen sollten daher genau bewerten, welche Form von Datenbank-Virtualisierung sie einsetzen. Sinnvoll ist es zudem, genau zu bestimmen, welche Daten sich für eine Auslagerung in die Cloud eignen. Auch der Service-Provider für DBaaS sollte mit Bedacht ausgewählt werden. Im Zweifelsfall besteht immer noch die Möglichkeit, einen derartigen Dienst in einer internen Private Cloud zu betreiben, bei der sich das Risiko-Management besser beherrschen lässt, da alle relevanten Parameter in der Hand des jeweiligen Unternehmens liegen. Besonders wichtig dabei ist die Exklusivität, mit der ausschließlich Daten des eigenen Unternehmens in der virtuellen Umgebung gehostet werden. Durch die Vermeidung von externen Usern in derselben Cloud-Umgebung lassen sich bereits viele Gefahren aussperren.

Drei zentrale Fragen, die Unternehmen vor Database-as-a-Service-Projekten klären sollten, sind:

- Welche Daten kommen für eine Auslagerung in Frage?
- Wer soll in der Datenbank auf welche Daten zugreifen können?
- Welche Form von Datenbank-Virtualisierung soll zum Einsatz kommen?

Martin Dombrowski
martin.dombrowski@imperva.com