Public Cloud: Lock-in-Risiko intelligent managen

Die Angst, sich auf Gedeih und Verderb einem Cloud-Service-Provider auszuliefern, hält viele Unternehmen von der vollen Nutzung des Potenzials einer Public Cloud ab. Dabei lassen sie sich jedoch Chancen entgehen, die durch intelligentes Risikomanagement genutzt werden könnten.

Bei der Nutzung der Public Cloud haben Unternehmen oft Bedenken, weil sie das Risiko eines Anbieter-Lock-ins fürchten. Sind diese berechtigt?

Risiken und Nutzen abwägen

Die Gefahr eines Lock-ins steigt mit dem Ausmass der Nutzung anbieterspezifischer Services. Oft bringen aber gerade die anbieterspezifischen Services auch Vorteile, da der Anbieter sich ja genau mit diesen von seiner Konkurrenz abhebt. Häufig steigt dieser Nutzen sogar, wenn mehrere solcher Services des gleichen Anbieters kombiniert werden, da diese optimal aufeinander abgestimmt sind. Es handelt sich also um einen Trade-off: Das volle Potenzial der Services eines Anbieter entfaltet sich umso stärker, je tiefer man sich in dessen spezifisches Ökosystem begibt; gleichzeitig nimmt aber auch der Lock-in zu.

Es gibt verschiedene Szenarien, in denen ein Lock-in gefährlich werden könnte. Diese sollten im Rahmen einer Risikoanalyse identifiziert und nach Wahrscheinlichkeit und Auswirkung bewertet werden. Daraus können entsprechende Massnahmen abgeleitet werden, von denen einzelne im Folgenden aufgezeigt werden.

Vertragliche Massnahmen aushandeln

Man sollte versuchen, mit dem Cloud-Anbieter möglichst gute Konditionen bezüglich einer ordentlichen sowie ausserordentlichen Kündigung auszuhandeln. Eine besondere Bedeutung kommt dabei dem Umfang und der Dauer der Leistungen zu, die der Anbieter nach einer ausserordentlichen Kündigung weiter zur Verfügung stellt.

Bild: Maksim Kabakou/ Fotolia.com

Der Autor
Dominik Langer, Chief Digital & Innovation Officer, Adesso Schweiz

Exit-Strategie entwickeln und Anbieter beobachten

Man sollte nicht nur eine initiale Due-Diligence-Prüfung des Anbieters durchführen, sondern vor der Nutzung von Cloud-Services auch eine Exit-Strategie für kritische Workloads entwickeln. Diese sollte eine periodische Risikoprüfung einschliesslich einer Beurteilung des Anbieters sowie relevanter Umfeldfaktoren vorschreiben. Ebenso sollte sie Massnahmen beschreiben, die bei erhöhtem Risiko eingeleitet werden müssen.

Beziehung zum Anbieter aufbauen

Beim Betrieb kritischer Workloads sollte man ein ausreichend hohes Supportlevel des Cloud-Anbieters nutzen. Je nach Anbieter kann die maximale Supportstufe einen dedizierten Technical Account Manager und die Möglichkeit beinhalten, Run Books zu definieren, die die Interaktion zwischen Cloud-Anbieter und -Nutzer bei einem kritischen Vorfall regeln. Daneben hilft es auch, auf Managementebene einen guten Draht zum Anbieter aufzubauen.

Architekturvorgaben etablieren und überwachen

Die Cloud-Architektur kann so gestaltet werden, dass kritische Anwendungen notfalls zu akzeptablen Bedingungen vom einen zum anderen Anbieter migriert werden können. Dazu sollten Services auf ihren Einfluss auf das Lock-in-Risiko und ihren Nutzen für das Unternehmen geprüft werden, bevor sie zur Verwendung freigegeben werden. Die Freigabe kann dabei auf bestimmte Applikationen beschränkt werden, etwa wenn der Nutzen für gewisse Applikationen zu klein oder das resultierende Lock-in-Risiko zu gross wäre. Manche Cloud-Anbieter stellen Services bereit, mit denen solche Vorgaben durchgesetzt und ihre Einhaltung automatisiert überprüft werden kann. Eine weitere Möglichkeit ist die Nutzung einer Abstraktionsschicht zwischen Cloud-Services und Applikationen, um die Migrierbarkeit zwischen verschiedenen Clouds zu erhöhen.

Zusammengefasst kann festgehalten werden, dass intelligentes Risikomanagement es erlaubt, den Nutzen zu maximieren, den man aus der Public Cloud ziehen kann, ohne dabei den Risikoappetit des Unternehmens zu verletzen.

«Gerade etablierte Unternehmen fürchten sich vor einem Lock-in»

Viele Unternehmen nutzen das Potenzial der Public Cloud nicht voll aus, unter anderem weil sie einen Lock-in-Effekt befürchten, kritisiert Dominik Langer, Chief Digital & Innovation Officer bei Adesso Schweiz. Interview: Colin Wallace

Welche Arten von Cloud-Services können das Lock-in-Risiko besonders erhöhen?
Dominik Langer: Ein Lock-in-Risiko entsteht insbesondere bei der Nutzung anbieterspezifischer Cloud-Services. Allerdings sind gerade die hinsichtlich Agilität und Innovationsfähigkeit besonders interessanten Serverless-Technologien von Hyperscalern oft recht anbieterspezifisch. Mit Serverless-Komponenten können einerseits mit Einsatz aktueller Technologien und mit minimaler betrieblicher Belastung innerhalb kürzester Zeit innovative, skalierbare und hochverfügbare Applikationen entwickelt werden, mit denen sich Unternehmen von der Konkurrenz abheben können. Andererseits steigt jedoch mit der Nutzung von Serverless-Diensten das angesprochene Lock-in-Risiko. Unternehmen müssen daher entscheiden, welchen Kompromiss sie zwischen der Minimierung ihrer Abhängigkeit von einem bestimmten Anbieter und der Maximierung ihrer Nutzung der von ihm angebotenen Dienste bereit sind zu akzeptieren.

Sollen Unternehmen einen solchen Entscheid überhaupt generisch fällen?
Eine gewisse allgemeine Richtung sollte mittels einer übergreifenden Cloud-Strategie vorgegeben werden. Ein strategischer Verzicht auf die Nutzung von Serverless-Komponenten kann aus Sicht der Wettbewerbsfähigkeit aber gefährlich sein. Hier kann es sinnvoll sein, etwaige architektonische Massnahmen zur Minderung des Lock-in-Risikos auf bestimmte Applikationen zu beschränken. In einer idealen Welt würde die Wahl für jede Applikation und jeden Cloud-Service sogar separat getroffen werden, abhängig von der Kritikalität der Anwendung, dem Nutzenversprechen eines bestimmten Dienstes, der Verfügbarkeit eines ähnlichen Dienstes bei einem alternativen Anbieter und dem Verhältnis zwischen der für die Migration benötigten und im Ernstfall verfügbaren Zeit.

Welche architektonischen Massnahmen gibt es, um das Lock-in-Risiko gering zu halten?
Wir können grob drei Kategorien unterscheiden. Erstens Governance-Massnahmen, welche die Nutzung anbieterspezifischer Cloud-Services einschränken. Zweitens die Nutzung einer Abstraktionsplattform, welche die Unterschiede zwischen einzelnen Anbietern möglichst weitgehend wegabstrahiert. Und drittens ein Multi-Cloud-Ansatz, bei dem man dem Lock-in-Risiko durch Diversifikation begegnet. Massnahmen aus den verschiedenen Kategorien können auch miteinander kombiniert werden.

Dominik Langer, Chief Digital & Innovation Officer bei Adesso Schweiz.

Welche Nachteile haben solche architektonischen Massnahmen?
Solche Massnahmen kosten im Aufbau und im Betrieb. Ausserdem führen sie dazu, dass man das Potenzial der Public Cloud nicht im vollen Umfang nutzt, quasi also mit angezogener Handbremse fährt. Dies führt zu Opportunitätskosten durch eingeschränkte Agilität und Innovationsfähigkeit. Gerade etablierte Unternehmen fürchten sich am meisten vor einem Lock-in-Risiko. Sie sind es aber auch, die sich am stärksten vor Disruption fürchten müssen. Neue Player am Markt sind diesbezüglich meist risikofreudiger und haben so gegenüber etablierten Unternehmen einen Wettbewerbsvorteil. Hier müssen sich Unternehmen fragen, welches Risiko sie stärker gewichten möchten: das Lock-in-Risiko oder das Risiko, vom Markt verdrängt zu werden. Ich persönlich glaube, dass es für Unternehmen je länger desto mehr ein existenzielles Risiko bedeutet, die Public Cloud nur halbherzig zu nutzen. Im Zentrum sollte daher immer die Frage stehen, ob die Gesamtkosten und sonstigen Implikationen solcher architektonischer Massnahmen in einem vernünftigen Verhältnis zu Eintrittswahrscheinlichkeit und Auswirkung der dadurch geminderten Risiken stehen.