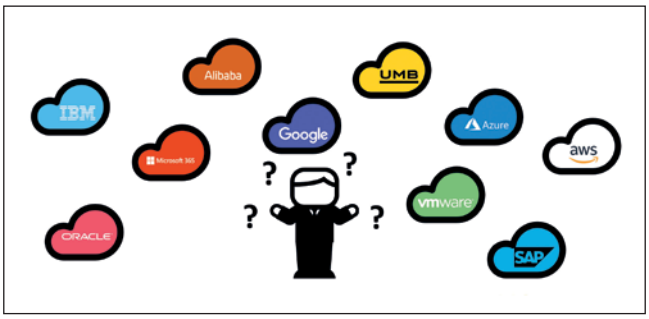
Unsicherheit bei Sicherheitsmassnahmen beseitigen

Know-how Wer seine IT in die Cloud auslagert, hat damit noch lange nicht seine Sicherheitsprobleme vom Tisch. Welche Anwendungen welche Vorkehrungen verlangen, ist abhängig von der Branche und der Risikobereitschaft des Unternehmens.

Von Von Felix Wolfensberger

Unternehmen, die heute ihre IT oder Teile davon in die Cloud auslagern, definieren damit eine wichtige Komponente der digitalen Transformation neu. Egal ob nun hybride oder Multi-Cloud-Konzepte mit privaten und öffentlichen Clouds gewählt werden und unabhängig davon, ob heutige Investitionen Zwischenschritte auf einem Weg ganz in die Cloud sind – die Basis für künftige Veränderungen wird heute gelegt. In der Diskussion um diese Weichenstellungen steht immer die Frage der Betriebsmodelle und Sicherheitsvorkehrungen, die gegeneinander abgewogen werden müssen. Dabei hängt die Entscheidung mehrheitlich von der Branche ab, in der ein Unternehmen tätig ist. Entgegen den Vorstellungen vieler Unternehmen und den Versprechungen der Anbieter ist mit der Auslagerung der IT in die Cloud nämlich die Sicherheitsproblematik nicht gelöst. Nach welchen Kriterien sollen IT-Entscheider also beim Outsourcing in die Cloud ihre Dienstleister prüfen?



Cloud-Leistungen gibt es in der Schweiz von den allergrössten der Branche bis hin zu kleinen KMU-Dienstleistern. Der Kunde hat die Qual der Wahl. Quelle: UMB

Regulierte Branchen

In den regulierten Branchen wie beispielsweise dem Bankensektor, dem Gesundheitswesen oder der öffentlichen Hand geben besondere Vorschriften und Gesetze hinsichtlich Sicherheit, Informations- und Datenschutz die zu treffenden Massnahmen vor. Sie gehen über die allgemeingültigen Datenschutzgesetze (EU-DSGVO, Schweizerisches Datenschutzgesetz etc.) hinaus. Organisationen, die sich in diesen Branchen bewegen, unterliegen entsprechenden Regularien, Banken und Versicherungen etwa den Auflagen der schweizerischen Finanzmarktaufsicht Finma. Lagern diese ihre IT aus, übergeben sie damit in der Regel auch die Verantwortung oder Teile davon an ihren Lieferanten. Dies zumindest was die physische Sicherheit angeht. Grundsätzlich kann man davon ausgehen, dass sich ein professioneller Cloud-Anbieter an die entsprechenden Vorgaben des Gesetzgebers hält. Anbieter, sei dies nun ein Lieferant einer SaaS-Lösung (Software as a Service) oder ein Plattformanbieter, können sich allerdings nicht etwa von einer Regulierungsbehörde zertifizieren lassen. Sie können sich lediglich von einem externen Auditor daraufhin (oder auf entsprechende ISO-Standards) prüfen lassen, dass sie nach den geltenden Regeln arbeiten. Hinzu kommt, dass auch die Umgebung, die die Kunden konfigurieren, den Kontrollen standhalten müssen. Dafür ist nicht der Cloud-Anbieter verantwortlich, sondern der Kunde. Hyperscaler bieten hierfür Compliance-Dashboards an, die den Konfigurationen gegenübergestellt werden können.

Finanz- oder Handelsunternehmen wiederum, die mit Kreditkarten als Zahlungsmittel operieren, müssen einen entsprechenden Branchenstandard, den PCI-DSS (Payment Card Industry Data Security Standard) erfüllen. Diesen Nachweis müssen sie auch erbringen, um zu beweisen, dass ihr IT-Dienstleister PCI-DSS-compliant ist und sie diesen regelmässig daraufhin prüfen. Hier geht es um Themen wie Firewalls, Passwörter, Datenschutz bei den Kreditkarteninhabern, aber auch Pflege der Sicherheitssysteme, Zugriffskontrolle und vieles mehr. Andere Unternehmen unterstehen keinen gesetzlichen Vorschriften, haben aber strenge Revisionspflichten. So müssen zum Beispiel bei Unternehmen im Bereich Vermögensverwaltung gewisse Sicherheitsstandards regemässig auditiert werden. Hier greifen Standards, die sich in den jeweiligen Branchen etabliert haben. So haben sich beispielsweise die Wirtschaftsprüfer auf den internationalen ISAE-Standard 3402 (International Standard of Assurance Engagements) geeinigt. In diesem ist die Prüfung eines internen Kontrollsystems bei Dienstleistungsunternehmen durch einen Wirtschaftsprüfer geregelt. Der Standard ist gerade

für solche Unternehmen respektive deren Outsourcer relevant. Auch sie lagern die Problematik an den Lieferanten aus, wenn sie ihre IT outsourcen. Aus der Verantwortung sind sie indes nicht, wenn beim Dienstleister Probleme auftreten. Viele Organisationen in regulierten Branchen nutzen deshalb, und weil teilweise nicht ganz klar ist, welche Daten ihrer Kunden zu den besonders schützenswerten gehören, die Public Cloud und deren Potential noch nicht vollständig aus oder verwenden deswegen Private Clouds. Hier bieten Service Provider Hand und beraten, wie und welche Clouds unter Berücksichtigung der regulatorischen Anforderungen optimal eingesetzt werden können.

ISO 27001 auch bei der Betriebsorganisation

Als richtungsweisend gilt sowohl für regulierte als auch unregulierte Branchen die ISO-Norm 27001, die die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems spezifiziert. Entscheidend ist dabei die Berücksichtigung des Kontexts und der Bedürfnisse der Organisation sowie die Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken. Hier geht es neben der erwähnten Sicherstellung der Konformität mit Gesetzen und Regularien um spezifische Ziele, um das Management von Sicherheitsrisiken, aber auch um die Identifikation und Definition von bestehenden und neuen Managementprozessen und Tätigkeiten im Zusammenhang mit Informationssicherheit. Entscheidend dabei ist, dass Anbieter daraufhin zu prüfen sind, auf welcher Ebene sie die Zertifizierungen erfüllen: Ist bei der Auslagerung in ein externes Rechenzentrum (Colocation) bloss die physische Sicherheit der Plattform zertifiziert oder auch die Betriebsorganisation selbst? Es geht also immer um die Rolle der verschiedenen Akteure: Wer macht Betrieb? Welches ist die Rolle der Hyperscaler, des Kunden und der Lieferanten? Und wie funktionieren die Schnittstellen? Dies sind Fragen, die bei der Beurteilung der Massnahmen zu prüfen sind.

Rechenzentren-Standards Tier 1-4

Bei Rechenzentren geht es bei den Qualitätsstufen Tier 1 bis Tier 4 um die Verfügbarkeit respektive die Ausfallsicherheit. Je nach Level unterscheiden sie sich hinsichtlich Systemtechnik, Energie-Effizienz, Datensicherheit aber auch der Verwaltungsorganisation in Sachen Leistungsfähigkeit. IT-Dienstleister begeben sich mit ihren Kunden in der Regel in die Obhut eines Rechenzentrumsanbieters und übernehmen damit dessen Qualitätsniveau. Allerdings spielen beim Cloud Computing die ersten zwei Level kaum eine Rolle: Die «Holzklasse» Tier 1 gewährt keine Redundanz und es besteht nur ein Energieversorgungweg. Tier 2 unterscheidet sich von Tier 1 hauptsächlich dadurch, dass redundante Komponenten verwendet werden. Tier 3 mit redundanten Komponenten, wie beispielsweis zweifach vorhandener Energieversorgung, Klimaanlagen sowie weiteren Versorgungswegen gewährt eine Ausfallsicherheit von 99,98 Prozent oder 1,6 Stunden pro Jahr – die Datacenter Facility ist fehlertolerant und wartungsfähig während des Betriebs. Die Meisterklasse Tier 4 wiederum bringt komplette Redundanz mit doppelten Versorgungswegen, sodass ein SPOF (Single Point of Failure) nahezu ausgeschlossen wird. Dass ein Bestandteil des Systems einen Ausfall des gesamten Systems nach sich zieht, ist praktisch ausgeschlossen. Die Verfügbarkeit beträgt 99,991 Prozent – die zu erwartende Ausfallsicherheit liegt unter einer Stunde pro Jahr.

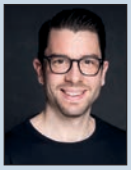
Datenzugang privilegieren

Die Qualitätsstufen von Rechenzentren sind allerdings heute nicht mehr das Kriterium bei der Definition der Vorkehrungen. Der Qualitätsunterschied zwischen Tier 3 und 4 ist für die meisten Unternehmen nicht relevant. Bei Unternehmen in nicht regulierten Branchen hängen die Sicherheitsvorkehrungen des Cloud-Anbieters vielmehr davon ab, welches Risiko ein Kunde tragen kann und will. Oder anders gesagt, wie lange der Ausfall bei einem Vorfall sein darf, um ohne grösseren Schaden davonzukommen. Die grosse Herausforderung der Unternehmen liegt also nicht so sehr im Nachweis von ISO-Zertifizierungen und Rechenzentrums-Standards. Absolut zentral bei der Sicherheitsproblematik hingegen ist die Transparenz im System. Es geht darum, zu wissen, wer auf welche Systeme Zugriff hat und diese so gut wie möglich einzuschränken. Mit Privileged Access Management (PAM) haben sich in der Vergangenheit Prozesse und Präventivsysteme etabliert, mit denen sich Risiken durch Mitarbeitende, Partner, Anbieter und Systeme reduzieren lassen. Mit dem Wechsel von On-Premises in die Cloud müssen aber vor allem die klassischen Zonen- zu Zero-Trust-Konzepten verändert werden. Denn in einer Cloud-Umgebung sind Sicherheitsarchitekturen komplett anders als bei klassischen Betriebsmodellen. Deshalb können die bestehenden Sicherheitskonzepte nicht eins zu eins in die Cloud transferiert werden.

Risikoabwägung und Sicherheitsmassnahmen

Bei den Security-Massnahmen, die zur Einhaltung der Datenschutzgesetze getroffen werden müssen, tappen die meisten Unternehmen im Dunkeln. Auch liegt es für die meisten Firmen in ihrer unternehmerischen Freiheit, welche Sicherheitsvorkehrungen sie umsetzen wollen. Hier helfen Risiko-Assessments. Wie gross ist das Risiko für Cyber-Angriffe? Sind Sicherheitsrichtlinien sinnvoll geregelt und werden sie auch eingehalten? Lücken und Schwachstellen, nicht nur in der Infrastruktur, sondern auch im Regelwerk und den Prozessen, müssen aufgezeigt und auf ihr potenzielles Risiko hin ausgewertet werden. Kann eine Firma einen Tag ohne IT auskommen? Was ist, wenn man mehrere Wochen brauchen würde, um den Betrieb wiederherzustellen? Braucht es ein Notfallkonzept, was der Kunde im Ernstfall zu tun hat? Oder müssen Risiken gar soweit reduziert werden, dass intelligente Technologien die Gefahren erkennen und automatisiert Massnahmen ergreifen, bevor Schaden entsteht? Aufgrund solcher Fragen können Massnahmen definiert und die Kosten abgewogen werden. Für Betreiber kritischer Infrastrukturen empfiehlt zum Beispiel das Bundesamt für wirtschaftliche Landesversorgung einen IKT-Minimalstandard. Er ist aber für jedes Unternehmen und jede Organisation anwendbar. ■

DER AUTOR



Felix Wolfensberger ist CSO - Head of Business Development & Sales beim auf Consulting, Cloud, digitale Transformation, Modern Work, Security und Infrastruktur spezialisierten IT-Dienstleister UMB.