Sandro Ineichen
Systemtechniker
(Wirtschaftsinformatiker HF)
IOZ AG
CH-6210 Sursee
T +41 41 925 84 00
sandro.ineichen@ioz.ch
www.ioz.ch

SICHERHEIT IN DER CLOUD – GEHT DAS ÜBERHAUPT?

Sandro Ineichen

Die Speicherung von Daten bei heutigen IT-Landschaften bringt zahlreiche Herausforderungen mit sich. Während früher alle Daten stets lokal gespeichert wurden, ist die partielle Ablage von Daten via Internet auf entfernten Servern (Cloud) nicht mehr wegzudenken. Entsprechende Anbieter von Cloud-Diensten sind Microsoft, Amazon, Google sowie zahlreiche kleinere Anbieter.

Die Begriffe Cloud und Sicherheit passen für viele Menschen jedoch nicht zusammen. Schon oft hat man von Angriffen – und damit verbundenen Datenlecks – auf Anbieter von Cloud Lösungen gehört. Schlagzeilen wie «Gehackte Cloud-Dienste: Angriffsziel Wolke» verunsichern Benutzer und IT-Mitarbeiter gleichermassen und schüren die Skepsis gegenüber Cloud-Diensten zusätzlich. Viele vergessen dabei, dass sie längst Teil der Cloud-Community sind, da sie «Public-Cloud»-Dienste wie Dropbox, iCloud oder Google Drive täglich nutzen. Die Cloud bietet auch im Business Umfeld Chancen: Die Sicherheit ist oftmals höher, als wenn sich eine Firma selbst an den Aufbau einer «Private Cloud» auf ihren Servern heranwagt. Eine weitere Variante, über die gerne gesprochen wird, ist die sogenannte «Hybrid Cloud», die es ermöglicht Daten sowohl lokal und/oder in der Cloud abzulegen.

Bedarf für «Cloud» klären

Private Cloud, Public Cloud oder Hybrid Cloud? Wofür soll man sich entscheiden? Bevor man sich überhaupt über Sicherheit und Datenschutz Gedanken macht, sollte zuerst geprüft werden, ob es sinnvoll ist, Dienste wie Kollaborationsplattformen, CRM oder auch Office Applikationen in die Wolke auszulagern. Ein Unternehmen stellt sich die Frage, wie das Thema Sicherheit in der Cloud anzugehen ist, wo die Gefahren lauern und welche Hürden es zu meistern gibt. Aspekte zur Sicherheit, Compliance sowie zu Governance und Datenschutz-Themen können beispielsweise in einer Aufklärungsplattform von Microsoft nachgelesen werden. Im sogenannten Microsoft Trust Center (https://www.microsoft.com/en-us/trustcenter) erfährt man zudem, dass Microsoft die Daten nicht für Werbezwecke missbraucht und die Daten jederzeit in Besitz des Kunden sind. Um diese Themen mit dem Kunden zu besprechen und zu behandeln, führt die IOZ AG ein sogenanntes Office 365 Readiness Assessment durch. So wird sichergestellt, dass alle die Voraussetzungen und Rahmenbedingungen kennen. Auch stellt sich die Frage, ob in Zeiten der Digitalisierung überhaupt noch auf die Cloud verzichtet werden kann. Der ortsunabhängige Zugriff auf Daten und das mobile Arbeiten sind lediglich zwei Vorteile. Des Weiteren sollte man sich den Schritt in die Cloud insbesondere dann überlegen, wenn die Anschaffung teurer Server-Infrastruktur bevorsteht.

IT-Security bedeutet Klärung organisatorischer Aspekte

Sehr oft sind sich Unternehmen nicht bewusst, dass eine Transformation in die Cloud nebst den technischen Massnahmen auch organisatorische Massnahmen mit sich bringt. Die IT-Security-Richtlinien in den Unternehmen erfüllen die Anforderungen an die neue Cloud-Infrastruktur oft nicht oder nur teilweise. Deshalb gilt es, diese bei einem Wechsel in die Cloud ebenfalls zu überdenken.

Oftmals ist die Kategorisierung der Daten und die Zuordnung des Schutzbedarfs ein erster Schritt, um die Richtlinien den neuen Gegebenheiten anzupassen. Typischerweise haben personenbezogene Daten wie zum Beispiel Personaldossiers besonders hohen Schutzbedarf und müssen deshalb gesondert behandelt werden.

Schritte zur Transformation in die Cloud

Je nach Schutzbedarf gibt es also Daten, welche sich für eine Speicherung in der Cloud eignen bzw. eben nicht eignen.

Nebst dem Schutzbedarf müssen die drei IT-Grundschutzziele Verfügbarkeit, Integrität und Vertraulichkeit ebenso überdenkt und gegebenenfalls angepasst werden.

Verfügbarkeit

Die Verfügbarkeit der Dienste muss vorab mit dem Anbieter des Cloud-Dienstes geregelt werden. Am Beispiel von Microsoft ist die Verfügbarkeit von Office 365 öffentlich bekannt, was Vertrauen schafft. Die weltweite Verfügbarkeit von Office 365 lag in den Jahren 2012/2013 bei durchschnittlich 99.97 % oder anders ausgedrückt bei einer maximalen Downtime von 13 Minuten pro Monat.

Integrität

Die Unverfälschbarkeit der Daten – die Integrität – wird in der Regel von Anbietern von Cloud-Diensten nicht garantiert. Der Nutzer respektive das Unternehmen, welches Cloud-Dienste einsetzt, muss hier selbstständig geeignete Massnahmen treffen, um die Integrität der Daten sicherzustellen.

Vertraulichkeit

Wie bei der internen Klärung des Schutzbedarfs, gilt es die Vertraulichkeit auch nach aussen zu berücksichtigen. Um diese zu gewährleisten, setzt bspw. Microsoft bei sämtlichen Office 365 Produkten auf eine SSL-verschlüsselte Verbindung.

Als weiteren Aspekt bringt eine Auslagerung in die Cloud einige sicherheitsbezogene Chancen mit sich: In einer lokalen Umgebung ist der Kunde jeweils selbst für die Ausführung von Updates und sicherheitsrelevanten Anpassungen verantwortlich. In der Cloud wird dieser Part teilweise durch den Betreiber übernommen und entlastet somit den Kunden. Bei Cloud-Diensten werden regelmässig und ohne dass es die Nutzer bemerken, Sicherheitsupdates eingespielt. Diese regelmässigen Updatezyklen und die damit verbundenen Sicherheitsoptimierungen reduzieren die Gefahr massiv, von aussen angegriffen zu werden.

Anwendung von IT-Security in der Praxis

Sind sämtliche cloudbezogenen Fragen geklärt und entsprechende Massnahmen umgesetzt, steht einer Transformation in die Cloud nichts mehr im Wege. Weitere IT-Security-bezogene Fragen stellen sich beim Aufbau der neuen Infrastruktur. Wie dies in der Praxis gelebt wird, zeigt folgendes Beispiel auf Basis von Microsoft Cloud Lösungen:

Mobilgeräte verwalten

Die Verwaltung von mobilen Geräten wie etwa Smartphones oder Tablets ist in der heutigen Zeit ein zentrales Thema. Viele Unternehmen setzen auf den «Bring Your Own Device»-Ansatz, was dem Thema zusätzliche Bedeutung verleiht. Die Verwaltung von eben solchen Geräten wird dadurch allerdings nicht gerade vereinfacht. Mit Microsoft Intune bietet der Gigant aus Redmond eine Verwaltungsplattform für Apps und Geräte an, welche nicht zuletzt dank der Cloud zahlreiche Sicherheitsfunktionen ermöglicht. Nebst Geräten mit Microsoft Betriebssystem können auch Geräte anderer Hersteller wie Apple oder Google verwaltet werden. Sei es nun bei der Verteilung von unternehmensspezifischer Software oder der Bereitstellung von Zertifikaten, WiFi-Einstellung, sicheren VPN-Verbindungen oder E-Mail-Profilen. Selbstverständlich bietet Intune auch einen integrierten Virenschutz. Zudem lassen sich die einzelnen Clients überwachen und verwalten. Die Frage nach fehlerhaften oder nicht installierten Updates lässt sich mit einem Blick in die Intune Verwaltungskonsole klären. Sollte ein Gerät abhandenkommen, so können die Daten mit wenigen Klicks unbrauchbar gemacht und vor unbefugtem Zugriff geschützt werden. Das Unternehmen behält somit die volle Kontrolle.

Nachrichten verschlüsseln

E-Mails sind von Experten so einfach zu lesen, wie eine Postkarte auf dem Weg zum Briefkasten. Die Verschlüsselung von Nachrichten ist deshalb nicht mehr nur ein «nice-to-have». Microsoft bietet seinen Nutzern auch hier unzählige Funktionen, welche die Anforderungen an Ihre Organisation hinsichtlich Sicherheit erfüllen. Mit Microsoft Azure Rights Management gibt es die Möglichkeit der Nachrichtenverschlüsselung. Damit werden E-Mails vollständig verschlüsselt, ohne dass der Empfänger hierfür einen Dienst abonnieren muss. Gegen Spam und Malware bietet Microsoft zudem mit Exchange Online ab Werk einen entsprechenden Schutz an.

Vertraulichkeit sicherstellen

Wie jeder Anbieter bleibt auch Microsoft nicht stehen und investiert massiv, insbesondere in die Sicherheit seiner Cloud Lösungen. Mit der Mehr-Faktor-Authentifizierung kann ein mehrstufiger Login-Prozess erzwungen werden, indem zum Beispiel ein weiteres Sicherheitskennwort auf dem Smartphone generiert und anschliessend in der Login Maske eingetragen werden muss. So kann sichergestellt werden, dass nur die berechtigte Person einen Zugang erhält. Ein weiteres immer wichtiger werdendes Thema ist das Schützen vertraulicher Informationen vor Ausdruck, Weiterleitung, Speicherung, Bearbeitung und Kopieren durch nicht autorisierte Benutzer. Das Zauberwort hierfür heisst IRM (Information Rights Management). IRM kann sowohl für Microsoft SharePoint Online als auch für Microsoft Exchange Online genutzt werden und lässt zu, dass Aktionen entsprechend eingeschränkt werden können. Beispielsweise kann definiert werden, wo welche Dokumente abgelegt werden dürfen. Ebenfalls verhindert werden kann das Lesen, Kopieren oder Drucken von Dateien und sogar das Herauskopieren von Text aus einer Datei. Unter anderem mit diesen Features lässt sich der benötigte Schutzgrad für Ihre Organisation erreichen.

Abschliessend lässt sich wohl sagen, dass Sicherheit in der Cloud keine Wunschvorstellung ist. Mit den heute zur Verfügung stehenden Mitteln kann ein Unternehmen den Wechsel in die Cloud durchaus wagen.