Sicher in die Wolken

Wie HiSolutions die Lufthansa Group beim Weg in die Cloud unterstützt

Es ist kein Geheimnis, dass heutzutage immer mehr Unternehmen die Cloud nutzen. Nur wenige deutsche Unternehmen wagen jedoch bisher den Schritt, ihre Kerngeschäftsprozesse in die Wolke zu schieben. HiSolutions unterstützt die Lufthansa Group auf diesem Weg der sicheren Migration in die Cloud.

Von Abdou-Naby Diaw, Deutsche Lufthansa AG, & Timo Kob, HiSolutions AG

Die Lufthansa Group setzt seit Jahren auf eine moderne IT-Landschaft mit einem gesunden Gleichgewicht zwischen Auslagerung und Eigenleistung sowie einer strategischen Governance, die die IT beständig den Geschäftsprozessen anpasst. Um den Herausforderungen der Zukunft noch effektiver, attraktiver und nicht zuletzt auch wirtschaftlicher begegnen zu können, wurde das Programm zur Modernisierung der IT-Infrastruktur ins Leben gerufen. Es umfasst unter anderem die Befähigung der Lufthansa Group, moderne Cloud-Technologie sicher zu nutzen und eine Basis für den Weg in die Digitalisierung zu legen. Dabei war von Anfang an selbstverständlich, dass neben Nutzerzentriertheit, Modernität und Wirtschaftlichkeit Security eine zentrale Rolle spielen muss. Daher wurde die HiSolutions AG beauftragt, die Lufthansa Group bei der sicheren Ausgestaltung der Cloud-Umgebungen zu unterstützen. Das Projekt umfasst sowohl strategische als auch operationale und technische Themen und verfügt über eine Vielzahl an Schnittstellen zu rechtlichen und Beschaffungsfragen.

Cloud-Strategie & Governance

Cloud-Nutzung hat unbestrittene Vorteile. Um jedoch auch das veränderte Risikoprofil managen und die Chancen optimal nutzen zu können, wurde der Weg in die Cloud von Anfang an mit einer Cloud-Strategie unterfüttert. Diese betrachtet wesentliche Compliance- und Legal Risks, spezifische Verfügbarkeitsrisiken von Cloud-Diensten und die Verteilung der Verantwortung zwischen Nutzern (Lufthansa Group und Tochtergesellschaften wie Swiss, Austrian Airlines, AirPlus und Brussels Airlines), Cloud-Anbietern und Dienstleistern. Ein zentrales Gestaltungselement ist die konsequente Ausrichtung auf eine Multi-Cloud-Strategie, mit der von Anfang an Gefahren wie Vendor-Lock-in und kumulierten Verfügbarkeitsrisiken entgegengesteuert wird. Für die Operationalisierung konnte beispielsweise auf das IT-Grundschutz-Kompendium des BSI zurückgegriffen werden, das Bausteine für Cloud-Nutzung und Cloud-Management bereitstellt. Ein weiterer Grundpfeiler ist Security by Default, die insbesondere aufgrund der Skalierbarkeit und Automatisierung an Bedeutung gewinnt.

Unterhalb der Strategieebene gliedert sich eine Vielzahl taktischer Themen an, die im herkömmlichen Betriebsmodell gut ausgestaltet sind, in der „neuen Welt“ jedoch neu beleuchtet werden müssen – und dabei Optimierungspotenzial bieten. Ein Beispiel ist der Payment Card Industry Data Security Standard: Sollen in der Cloud Kreditkartendaten

verarbeitet werden, ist eine Zertifizierung nach PCI DSS erforderlich. Zwar muss diese alle kartenverarbeitenden Dienste abdecken, jedoch kann ein geeignetes Cloudangebot viele Anforderungen bereits erfüllen, sodass nur das jeweilige Delta umgesetzt werden muss.

IAM in der Cloud

Active Directory (AD) bleibt auch in der Cloud das zentrale Instrument für Identity- und Access-Management – mit mehr Möglichkeiten: Neben einem dedizierten Azure AD ist auch der Betrieb eines herkömmlichen AD auf Cloud-Ressourcen möglich oder aber ein (Teil-)Betrieb des IAM on premises. In Abwägung aller Schutzziele und Risiken ist es gelungen, für die Lufthansa Group ein Konzept zu entwickeln, bei dem alle Cloud-Assets und Nutzer in der Cloud verwaltbar sind, während gleichzeitig hochprivilegierte Verwaltungs-Assets noch stärker geschützt sind. Dafür war die Anpassung des ESAE-Konzepts von Microsoft (Enhanced Security Administrative Environment) auf Azure und die Abbildung der Cloud-Landschaft auf eine 3-Schichten-Architektur (engl. 3-Tier) notwendig.

Container-Security

Ihre volle Stärke können Cloud-Dienste entfalten, wenn sie automatisiert werden. Cloudanbieter bieten heute komplexe Container-Techniken wie Kubernetes an, die flexible Orchestrierung von Diensten ermöglichen und idealerweise die Entwicklung agiler und Ressourcen skalierbarer machen. Allerdings gibt es noch kaum Standardrezepte für die Security. Es geht also darum, Vorgaben für einen sicheren Rahmen zu machen, ohne Flexibilität und Agilität zu zerstören.

Zudem gilt es, Assets zu härten, die immer wieder Verwendung finden, sei es als „nackter" Server, Domänencontroller oder Kubernetes-Host. Hierfür haben sich die CIS-Benchmarks (Center for Internet Security) als angemessene, umfassende Basis erwiesen.

Das Kleingedruckte

Auch juristisch gibt es beim sicheren Weg in die Cloud vieles zu beachten. So beschreiben übliche Cloud-AGBs eine Vielzahl rechtlicher Eigenschaften und referenzieren dabei teilweise auch auf objektive Eckpunkte wie DSGVO oder PCI DSS. Um ein Mapping zum Anforderungsprofil der Lufthansa Group herzustellen, hat das Projektteam die AGBs von Cloud-Diensten systematisch untersucht und mit den internen Richtlinien abgeglichen, um die Compliance auch auf dieser Ebene sicherzustellen.

Eine besondere Rolle spielen dabei Standards, die den Anbietern wahlweise als Gütesiegel oder aber als Verweis auf Anforderungs-Sets dienen. Entscheidend ist, welche Normen welche Qualität verlässlich nachweisen können. Wirbt ein Anbieter etwa mit einer ISO-27001-Zertifizierung für seine Container-Services, so ist dies kein substanzielles Versprechen, da der Standard für den Anwendungsbereich wenig Spezifisches enthält. ISO 27017, ISO 27018 und der BSI-Anforderungskatalog Cloud Computing (C5) hingegen können für bestimmte Teilbereiche sinnvolle Vorgaben darstellen.

Vieles, was im Zuge des Programms passiert, ist in der Größenordnung, wie die Lufthansa Group es vorantreibt, Neuland im Bereich der IT-Strategie und -Umsetzung. Daher ist ein gewisser Grad an Offenheit und Vertrauen notwendig, dass das, was zwischen Managed Service Provider und Lufthansa Group als Kunde geschieht, im beiderseitigen Nutzen optimal beschrieben ist. Tools, die dies – auch in Bezug auf Security – sicherstellen, sind ein Framework-Agreement sowie umfangreiche Statements of Work (SoWs), die einerseits modular auf klassischen IT-SoWs aufbauen, andererseits aber anbieterneutral speziell für Cloud entwickelt wurden, wo klassische SoWs keine Anwendung finden können. Security-Anforderungen wurden in einem Wechsel aus Breakout-Sessions und Konsolidierungsrunden kooperativ integriert.

Lessons Being Learnt

Im Rahmen des Programms stellen sich auch für die Security immer wieder neue Herausforderungen, etwa die notwendige Ungleichzeitigkeit von Prozessen aufgrund der Agilität des Vorgehens und der notwendigen starken Parallelisierung. Hier ist die Flexibilität aller Beteiligten der Schlüssel zum Erfolg, zunächst Mut zur „Lücke" im Sinn von Grob(st)konzept zu beweisen, um dann in weiteren Iterationen die Details herauszumeißeln. Das alte Wasserfallmodell der Architektur war nicht immer ausreichend flexibel – beim Thema Cloud erweist es sich als vollends ungenügend.

Die zweite Lektion besteht darin, frühzeitig alle Stakeholder an alle relevanten Tische zu holen. Es mag an vielen Stellen zunächst mehr Zeit kosten, Security-Fragen auch mit dem Einkauf oder dem Datenschutz zu diskutieren, jedoch erkauft man sich damit später Synergiemöglichkeiten, wenn Verhandlungen nicht neu aufgemacht werden müssen, weil etwa ein Tochterunternehmen hinzukommt.

Dank der intensiven Zusammenarbeit des IT-Security-Bereiches der Lufthansa Group und HiSolutions ist sichergestellt, dass die Security voll berücksichtigt ist im Sinne des Security-by-Design- und -by-Default-Ansatzes.

Abdou-Naby Diaw ist CISO und VP Cyber Security & IT Cross Functional Processes der Deutschen Lufthansa AG.

Prof. Timo Kob ist Vorstandsmitglied der HiSolutions AG.