Cloud Service – Himmel und Hölle

Alexander Weber, Firma e:ndlich

Dieser Erfahrungsbericht stellt zunächst den Oracle Cloud Schema Service vor und zeigt dann die Aufgaben während der Migration. Es folgt ein Einblick in eine Phase der Nutzung, die zu einer massiven Störung des Geschäftsbetriebes führte und somit die möglichen Schwachstellen eines Cloud Service offenbart. Abschließend sind die Vor- und Nachteile dieses Cloud Service gegenübergestellt.

Seit mehr als fünf Jahren ist das Thema „Cloud" in aller Munde und die Firma „endlich" hat sich deshalb frühzeitig entschieden, hier selbst Know-how aufzubauen. Es gab zwei wichtige Gründe, sich mit den Cloud Services zu beschäftigen. Erstens, um den Aufwand der selbst betriebenen Infrastruktur zu minimieren. Zusätzlich sollten die Verfügbarkeit gesteigert und der Betrieb stabiler werden. Die zweite Motivation war ein großes Interesse daran, sehr früh eigene Erfahrungen in der Anwendung von Cloud Services zu sammeln.

Welchen Cloud Service?

Prinzipiell gibt es mehrere Ansätze, einen Cloud Service zu wählen. Eine Möglichkeit ist, alles so zu nehmen, wie es ist, entsprechende Maschinen in der Cloud zu abonnieren und alles „1:1" zu übertragen. Dieser Ansatz ist jedoch nicht wirklich eine Verbesserung, da man eigentlich nur den Spielplatz wechselt, die Spielzeuge aber gleich bleiben. Dies kann sinnvoll sein, wenn man ohnehin mit seinem bisherigen Betreiber unzufrieden ist und wechseln will.

Eine zweite Option ist es, die Hardware zu virtualisieren und einige vorhandene

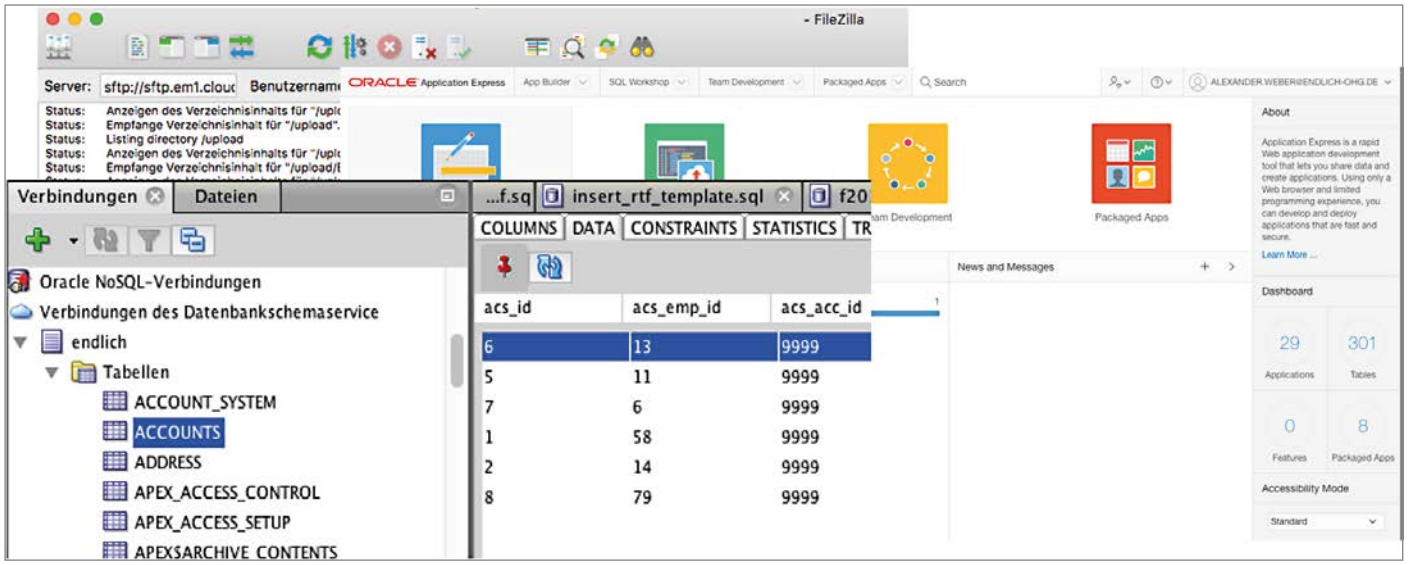

Abbildung 1: Ausschnitte aus den Cloud-Service-Zugängen mit Apex, FileZilla und SQL Developer

Dienste in die Cloud zu verlagern (etwa eine Datenbank oder ein Active Directory), damit geht man schon in Richtung Konsolidierung und Standardisierung der eigenen Anwendung.

Die dritte Möglichkeit besteht darin, einen Service zu wählen, der es ermöglicht, dass die eigene Anwendung ausschließlich auf Basis von Cloud Services läuft und man sich wirklich nur noch um den Betrieb und die Weiterentwicklung der Anwendung kümmern muss.

Als letzte Alternative bliebe noch die vollständige Ablösung der eigenen Anwendung durch eine Cloud-Lösung, die annähernd dasselbe macht wie die selbstentwickelte Lösung und bei der man sich danach nicht mehr um die Weiterentwicklung kümmern muss.

Das Unternehmen des Autors hatte zum Zeitpunkt der anstehenden Entscheidung für einen Wechsel in die Cloud viele Anwendungen im Haus, die auf Oracle-Basis und im Frontend auf Apex liefen. Der maximal unterstützte Technologie-Stack wurde von Oracle selbst angeboten, denn hier erhielt man einen Service, der sich sogar um den Betrieb und die Pflege von Apex kümmert. Die Wahl fiel deshalb auf den Oracle Cloud Schema Service.

Der Oracle Cloud Schema Service

Dieser Service läuft unter der Kategorie „Platform as a Service" (PaaS). Man bezeichnet so eine Dienstleistung, die in der Cloud eine Computer-Plattform für Entwickler von Webanwendungen zur Verfügung stellt. Dabei handelt es sich um schnell einsetzbare Laufzeit-Umgebun-

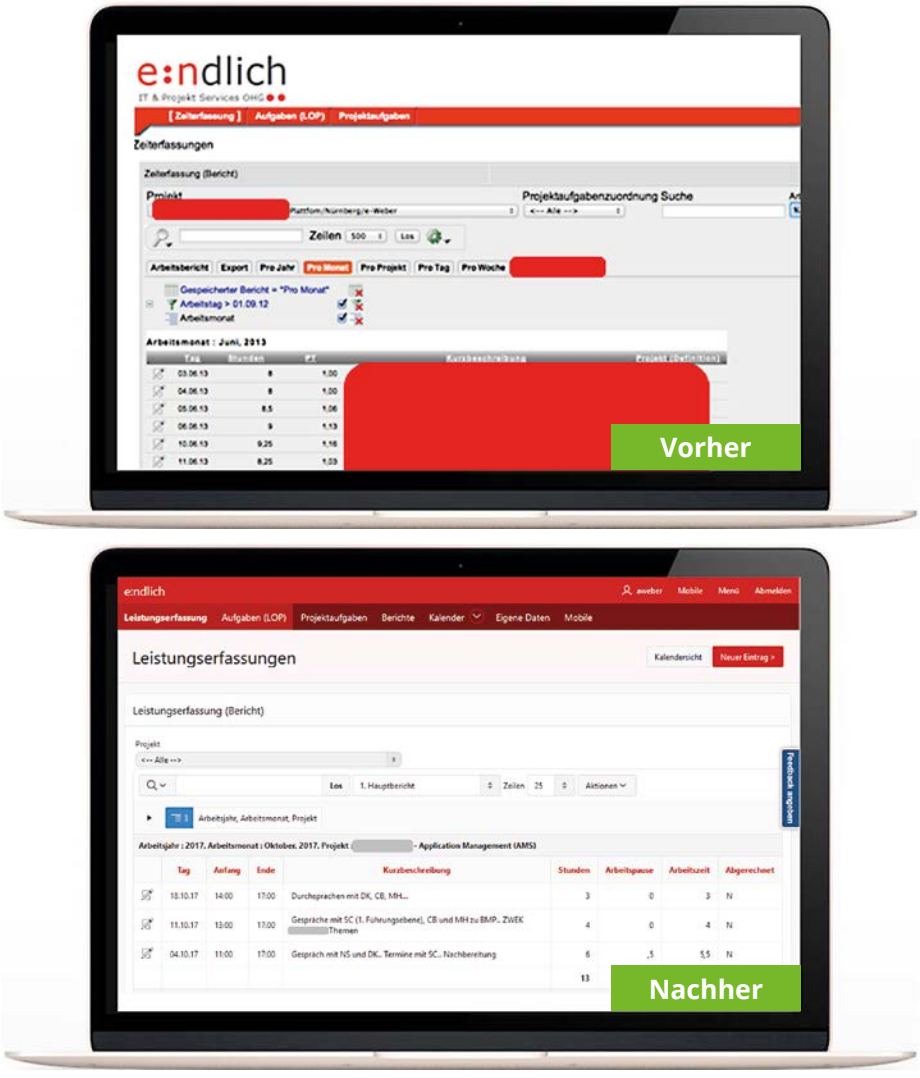

Abbildung 2: Teilmodul „Leistungserfassung" vor und nach der Migration in die Cloud

gen, aber auch um Entwicklungs-Umgebungen, die mit geringem administrativen Aufwand und ohne Anschaffung der darunterliegenden Hard- und Software genutzt werden können *(siehe Abbildung 1)*.

Der Database Schema Service besteht derzeit aus:

- Apex 5 (5.1.3), zum Zeitpunkt der Migration war es Apex 4 (4.2.6)
- Ein Datenbank-Schema auf einer 11g R2 Datenbank (11.2.4)
- SFTP-Zugang für Export/Import
- Zugang zu den Daten über REST-Services (zum Beispiel auch über SQL Developer)

Entwickler nutzen PaaS, um neuartige und bewusst für die Cloud gestaltete Applikationen zu entwickeln. Dabei stehen einem prinzipiell alle Micro-, REST-, Web- und Cloud-Services zur Verfügung, um die Anwendung zu erweitern. In sogenannten „Marketplaces" kann man diese auch gut vermarkten.

Die Umsetzung/Migration

Im ersten Schritt ging es darum, eine geeignete Applikation für die Migration in die Cloud zu finden. Das Team des Autors hat folgende Kriterien zugrunde gelegt:

- Möglichkeit der Konsolidierung der Anwendung auf die Zwänge der zukünftigen Ziel-Umgebung ist mit hoher Wahrscheinlichkeit vorhanden
- Bereitstellung eines Entwicklers aus bestehenden Projekten für diese Anwendung ist möglich. Es sollte jemand sein, der die Anwendung (mit-) entwickelt hat und sie sehr gut kennt
- Möglichst keine Verzahnung mit anderer Software und wenige Schnittstellen

Die Wahl fiel auf die Apex-Anwendung zur Unternehmenssteuerung, also quasi ein ERP-System *(siehe Abbildung 2)*.

Folgende Aufgaben standen auf der To-do-Liste:

- Konsolidierung und Re-Engineering der Anwendung
- Migration Apex 3 nach Apex 4 (damals)
- Zusammenführung des Daten- und des Applikations-Schemas
- Obfuscation-Toolkit durch „DBMS_CRYPTO" ersetzen

Abbildung 3: Datenschutz

- Deployment-Vorgehen anpassen
- LDAP-Bezüge eliminieren
- Java-Reports-Engine durch eine PL/SQL-Eigenentwicklung ersetzen
- Neue Application-IDs

Datenschutz

Der Datenschutz spielt im Cloud-Umfeld eine große Rolle. Kunden in Deutschland und Europa legen viel Wert darauf, dass mit ihren Daten sorgsam umgegangen wird, was gleichzeitig ein gewisser Innovations-Hemmschuh ist. Das Unternehmen des Autors hat sich deshalb mit den Gesetzen und Bestimmungen auseinandergesetzt und frühzeitig einen externen Datenschutzbeauftragten ins Boot geholt, um Fragestellungen bezüglich IT-Sicherheit und Datenschutz zu begleiten *(siehe Abbildung 3)*.

Mit Datenschutz ist in der Regel auch gleichzeitig IT-Sicherheit gemeint, was jedoch nicht dasselbe ist. Es gibt im Zusammenspiel von Datenschutz und IT-Sicherheit jedoch eine Überschneidung durch die technisch-organisatorischen Maßnahmen (TOM). Bei einer Migration von Services in die Cloud sind sowohl die eigenen TOMs als auch die des Cloud-Anbieters unter die Lupe zu nehmen. Dies betrifft insbesondere die Auftragsdatenverarbeitung.

Beim Datenschutzgesetz (BDSG beziehungsweise EU DSGVO) geht es darum, die Daten von natürlichen Personen zu schützen. Dazu zählen Attribute wie Name, Vorname, Geburtstag, Geburtsort etc., aber auch die näheren personenbezogenen Daten wie Straße und Ort oder BIC und IBAN. Es geht darüber hinaus auch immer darum, ob man mithilfe der Daten in einem Datenpool einen Bezug zu einer Person herstellen kann oder nicht.

Eine Datenmenge gilt rechtlich als datentechnisch verschmutzt, wenn es einen Datensatz gibt, mit dessen Hilfe eine Person eindeutig identifizierbar ist. Als Beispiel: In einem Datenpool werden lediglich Ortsteil und Alter gespeichert und ausgewertet. Dies klingt erst mal unkritisch, allerdings könnte es sein, dass im fiktiven Ortsteil „Einsamer Hof in kleiner Stadt" nur ein einziger Mensch mit 85 Jahren wohnt, weshalb man direkt Rückschlüsse auf die Person ziehen könnte – was nicht erlaubt ist.

Im IT-Sicherheitsgesetz steht der Schutz kritischer Infrastrukturen im Vordergrund, die beispielsweise für die Wasser- und Energieversorgung oder die Aufrechterhaltung des Gesundheitswesens verantwortlich sind. Wenn man Systeme für solche Infrastrukturen zur Verfügung stellt, muss man auch dafür Sorge tragen, dass die IT-Sicherheit gewährleistet ist. Hier liegt ein klarer Vorteil in der Nutzung von Cloud-Diensten, da diese in vielen Fällen den Anforderungen der IT-Sicherheit von vornherein genügen.

Gemäß § 9 Bundesdatenschutzgesetz (BDSG) sind alle Stellen, die personenbezogene Daten verarbeiten, erheben oder benutzen, verpflichtet, technische und/oder organisatorische Maßnahmen zu treffen, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind, etwa die Zugangs- oder Auftragskontrolle. Sie müssen die Einhaltung der TOMs selbst laufend kontrollieren, aber auch beim Cloud-Anbieter nachfragen.

Was ist mit den US-Anbietern?

Jene US-Anbieter, die einen Großteil der Cloud-Service-Angebote stellen oder die Hersteller der zugrunde liegenden Software sind, unterliegen per se nicht den Datenschutz- und IT-Sicherheitsbestimmungen der EU. Allerdings gab es dafür in der Vergangenheit das Safe-Harbour-Abkommen und nun das „EU-U.S. Privacy Shield", eine Art Freibrief, der es erlaubt, die US-Dienste zu nutzen.

Grundsätzlich ist es hilfreich, wenn man einen Cloud-Dienst-Anbieter mit europäischer Niederlassung wählt, da dieser somit auch auf europäischem Boden betrieben wird. Bei dieser Konstellation gelten die europäischen Gesetze und Richtlinien auch für den US-Anbieter.

Oracle hat weltweit lokale Data-Center in Betrieb. Das Unternehmen des Autors hat sich damals für das Datacenter „EMEA1" auf schottischem Boden in Linlithgow entschieden. Viele Informationen über das Data-Center werden jedoch nicht bereitgestellt. Auch online etwas darüber herauszufinden, ist nicht leicht, was jedoch potenzielle Angriffe wegen fehlender Informationen erschwert. Man bewertet das deshalb nicht als negativ.

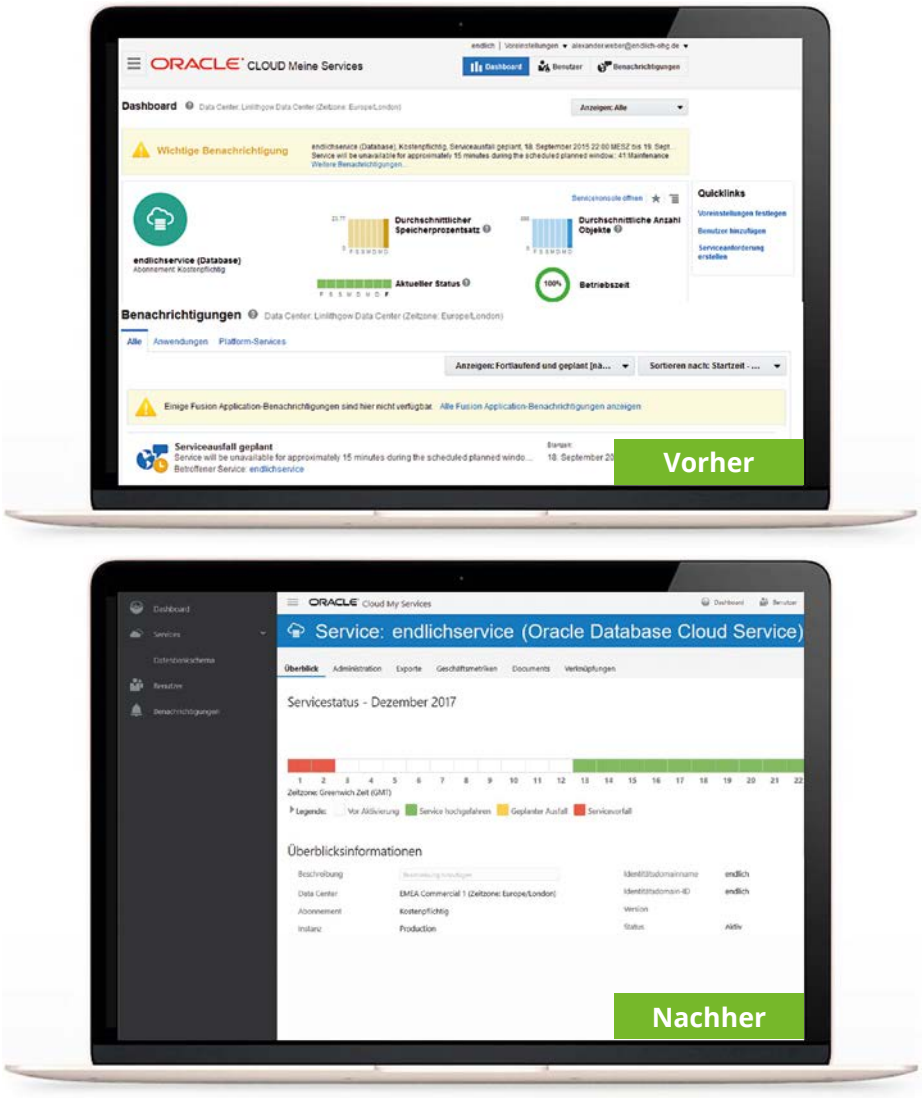

Abbildung 4: Service-Ansicht vor zwei Jahren und heute

Datenschutz-Fahrplan für den Weg in die Cloud

Folgende Punkte sollten auf jeden Fall implementiert sein, bevor man eigene Services in die Cloud migriert:

- Es sind externer Datenschützer und interner Datenschutzbeauftragter zu benennen
- Cloud-Anbieter-TOMs sind durch externe Datenschützer abgefragt und existieren
- Cloud-Dienst erfüllt BDSG beziehungsweise die EU-DSGVO
- Cloud-Anbieter ist nach ISO 27001 zertifiziert
- Data-Center befindet sich innerhalb der EU oder/und es existiert ein Angemessenheitsbeschluss wie das „EU-U.S. Privacy Shield"

Wie sich der Service überwachen lässt

Sobald die Anwendung in der Cloud ist, hat man auch ein Interesse daran zu wissen, wie der Dienst funktioniert. Es gibt dazu ein „Cloud Service Dashboard", in dem alle Cloud-Dienste aufgelistet sind. Dort lassen sich für jeden Service die wichtigsten Parameter wie Speicherplatz-Nutzung, Verfügbarkeits-Status in der aktuellen Woche und die generelle Betriebszeit ablesen. Es sind zudem einige grundsätzliche Verwaltungsaktionen (wie die Benutzerverwaltung und die Initiierung von Datenexporten) möglich. Ein Datenexport wird manuell beauftragt und kann kurz darauf vom SFTP-Server abgeholt werden. Inzwischen bekommt man auch proaktive Informationen über geplante Ausfallzeiten in der Service-Ansicht und separat als E-Mail *(siehe Abbildung 4)*. Das Look & Feel des Dashboards und auch die Service-Ansicht haben sich in den letzten Jahren mehrmals verändert, was es immer etwas anstrengend macht, sich zurechtzufinden.

Im Himmel

Nachdem das Unternehmen migriert hatte, ist man zu der Überzeugung gelangt,

dass der Aufwand von einem halben Jahr, um die Anwendung zu migrieren, auf jeden Fall gerechtfertigt war. Verglichen mit der Energie, die man vorher täglich in die Betreuung der Applikation investieren musste, ist der jetzige Zustand der Himmel des Anwendungsbetriebs. Vor allem folgende Vorteile standen im Vordergrund:

- Keine Betriebsaufgaben mehr
- Ab der Migration deutlich weniger ungeplante Ausfallzeiten
- Apex-Backend-Migrationen werden für das Unternehmen durchgeführt
- CPUs und/oder PSUs werden für das Unternehmen eingespielt
- O/S-Patches werden für das Unternehmen eingespielt
- Angriffe von außen werden abgewehrt
- Das Unternehmen kümmert sich nur noch um die Entwicklung
- Statt einer Datenbank-Lizenz und jährlichen Support-Kosten nun ein monatlich kündbares Abonnement
- Von Anfang an skalierbar

Hölle – oder was dann geschah

Bei der Cloud-Anwendung handelt es sich um die firmeninterne ERP-Anwendung zur Verwaltung der Angebote, Aufträge, Rechnungen, Assets, Mitarbeiterdaten und Leistungserfassung. Sie ist Dreh- und Angelpunkt des Geschäfts. Die Mitarbeiter nutzen die Anwendung beim Kunden, um ihre verrechenbaren Leistungen zu erfassen, Mitarbeiter im Backoffice erfassen mithilfe der Anwendungen neue Aufträge, erstellen Rechnungen, verwalten die Assets und es werden Dokumente zu Mitarbeitergesprächen verschlüsselt hinterlegt.

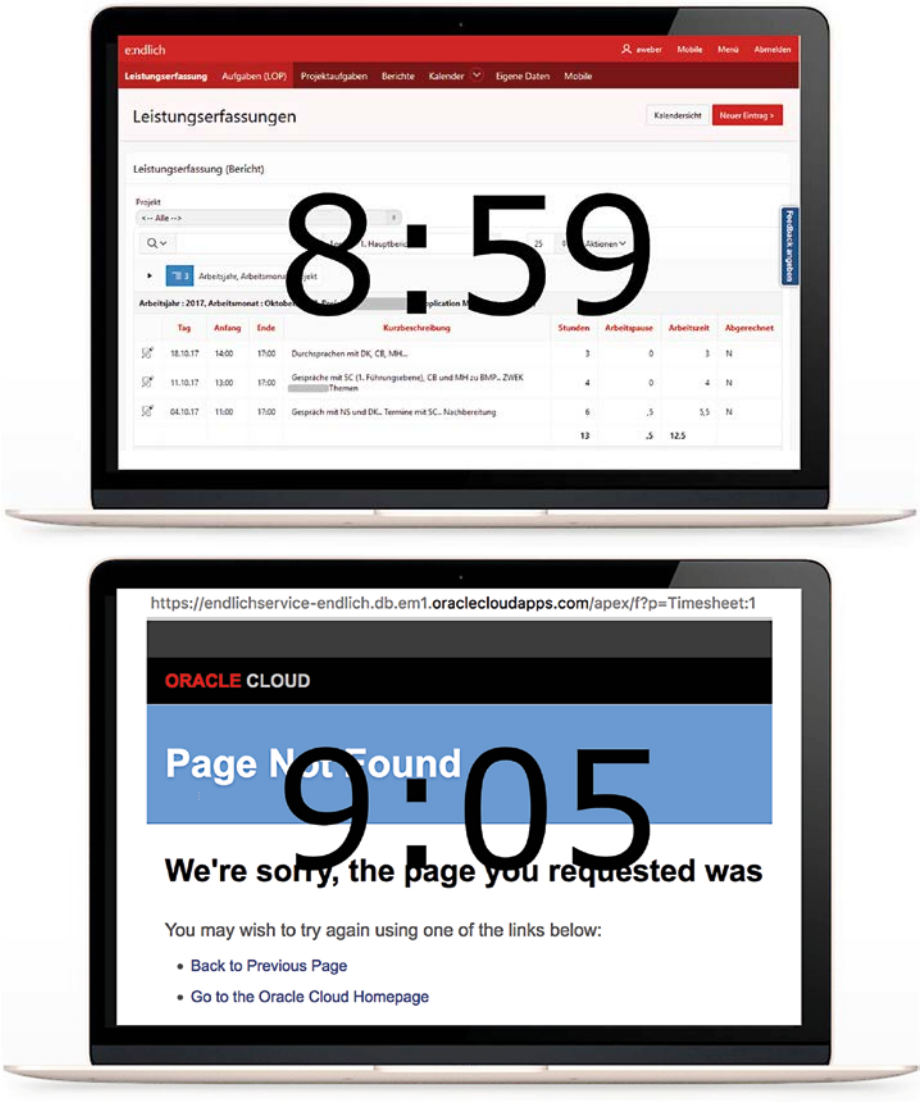

Abbildung 5: Anwendung in der Cloud nicht mehr verfügbar

Im Februar 2017 stand jedoch die Anwendung von der einen auf die andere Minute nicht mehr zur Verfügung *(siehe Abbildung 5)*. Nach einer kurzen Wartezeit wurde ein PRIO-1-Service-Request bei Oracle eröffnet und man hoffte auf eine zügige Bearbeitung.

Zur Erinnerung: Ein PRIO-1-Service-Request ist die höchstmögliche Priorität, mit der man einen Service-Request absetzen kann. Bei der Eröffnung eines solchen Tickets muss nicht nur der Fehler beschreiben, sondern es müssen auch die Ansprechpartner, die Manager und jeweils deren Kontaktdaten benannt sein. Diese sollen dann für Oracle rund um die Uhr zur Verfügung stehen beziehungsweise erreichbar sein. Somit wurde ein klares Signal gesetzt, dass es sich um ein wichtiges Anliegen handelt und zeitnahe Unterstützung erforderlich ist. Die erste Reaktion seitens Oracle war deshalb sehr enttäuschend: „Hi Alexander, we don't support Apex Cloud Service issues. Please reach out to the right team. Regards, … Oracle Cloud Services …"

Man wurde jedoch nicht informiert, welches das richtige Team ist, und der Ball lag wieder beim Unternehmen; man wurde quasi abgewimmelt, was sich in dem Augenblick nicht gut anfühlte. Das Unternehmen führte zeitgleich Telefonate mit Oracle-Support, Oracle Potsdam und Oracle München. Es stellte sich heraus, dass es für den Support gar nicht so leicht zu ermitteln ist, um welchen Cloud-Dienst es eigentlich geht. Die Abo-ID und die CSI-Nummer reichten dazu jedenfalls nicht aus. Man wurde gebeten, Schema- und Tablespace-Name zu benennen – das ist jedoch nicht so einfach, wenn der Service nicht mehr zur Verfügung steht.

Mit etwas Glück und durch Recherche in Skripten konnte man die gewünschten Informationen zusammentragen. Zwischenzeitlich wurde das zuständige Support-Team identifiziert („CLOUDOPS"). Es hat für das Unternehmen jedoch ziemlich intransparent im Hintergrund gearbeitet. Der Kontakt im Support konnte Fragen nicht direkt beantworten, sondern musste diese erst an das CLOUDOPS-Team weiterleiten.

Das Unternehmen wurde parallel durch den vertrieblichen Ansprechpartner gebeten, einen neuen Database Schema Service

zu bestellen. Wozu dies nötig war, konnte man zu dem Zeitpunkt nicht begreifen, hat es aber aufgrund der Notlage getan. Dies ging letztlich relativ schnell, allerdings musste man als kleinere Firma auch nicht über einen Einkauf gehen und zeichnungsberechtigte Personen finden, sondern konnte alles durch die Geschäftsführung erledigen lassen. Zwei Tage nach Eröffnung des Service Request stand der neue, völlig nackte Cloud Schema Service zur Verfügung. Nackt deshalb, weil dieser Service weder unsere Daten noch unsere Anwendung enthielt.

Nun traf ein weiterer Rückschlag seitens des Supports ein. Nachdem man bestätigt hatte, dass der neue Cloud-Dienst grundsätzlich zur Verfügung steht, kam folgende Antwort: „Hi, Thanks for your confirmation. I will be closing this SR since the service is active now. For any issues, kindly log a separate SR. Kind Regards,…"

Man fühlt sich in diesem Augenblick sehr einsam und bereut zutiefst, jemals die Entscheidung pro Cloud getroffen zu haben. Dieses Beispiel unterstreicht den Beitrag von Herrn Dr. Neugebauer „Oracle Support – Quo vadis" Anfang des Jahres im Red Stack Magazin, in dem er die sinkende Zufriedenheit mit My Oracle Support anspricht.

Das Unternehmen hat im Anschluss direkt mit dem Produktmanagement Kontakt aufgenommen und ab diesem Zeitpunkt den Eindruck, dass tatsächlich etwas passiert. Nach und nach standen immer mehr Daten aus der gewohnten Umgebung zur Verfügung. Zunächst erstmal nur der Zugriff auf die Laufzeit-Umgebung, aber es waren immerhin wieder die eigenen Daten zu sehen und die Anwendung hat grundsätzlich funktioniert. Es wurden jedoch unter anderem noch Umlaute in der Applikation falsch dargestellt und Public beziehungsweise Private Interactive Reports waren nicht verfügbar.

Auch der Zugriff auf die Apex-Entwicklungsumgebung war nicht möglich. Aber: Das Schlimmste war zunächst überstanden und das Unternehmen hat sich bei den hilfreichen Unbekannten über das Produktmanagement bedankt. Es kam folgende Antwort: „… Kollegen in den USA haben in einer konzentrierten Aktion mit diversen anderen Cloud-Teams das Ganze wiederherstellen/mit alten Namen aufsetzen können …"

Fünf Tage später konnte man also wieder grundsätzlich mit der Anwendung arbeiten und der Geschäftsbetrieb war nicht mehr eingeschränkt. In der Folgezeit wurden auch alle weiteren Schwierigkeiten gelöst, es gibt inzwischen wieder ein völlig sauberes System und man kann wie zuvor damit arbeiten.

Eines zeigt diese Antwort des Cloud-Service-Produktmanagements jedoch auch: Die Komplexität, einen versehentlich gelöschten Service wiederherzustellen – und bei diesem Beispiel handelt es sich nicht um eine komplexe Umgebung – ist offenbar sehr hoch und bedarf der Zusammenarbeit mehrerer Spezialisten.

Eine wirklich offizielle Ursache für diesen Ausfall hat das Unternehmen nie erfahren, konnte aber den Gesprächen Folgendes entnehmen: Der Cloudvertrag basierte auf einer Kreditkarte, deren Ablaufdatum im August des Vorjahres erreicht war. Es gab jedoch keine Kommunikation seitens Oracle darüber, dass dies der Fall ist. Der Service lief trotzdem von August des Vorjahres bis Februar weiter und wurde dann irgendwann auf „zu archivieren" gestellt; die technische Ausführung dazu fand im Februar statt.

Fazit

Letztendlich lässt sich sagen, dass die Ursache für den Ausfall kein technischer Fehler des Cloud Service, ungewollter Datenverlust oder Hackerangriff war. Es handelte sich um ein Problem in den Verwaltungsprozessen, die den Cloud Services zugrunde liegen. Bei komplexen, multinationalen Strukturen in großen Konzernen, bei denen die Prozesse nicht mit den technischen Innovationen Schritt halten können, kann dies zu Problemen führen. Es ist deshalb notwendig, einen funktionierenden Kommunikationskanal zwischen den Nutzern von Cloud-Diensten und dem Anbieter herzustellen, der während des gesamten Application Lifecycle einer Cloud-basierten Anwendung funktioniert. Dies könnte der Support sein, ist es aber derzeit nicht.

Trotzdem überwiegen für uns insgesamt die Vorteile, die die Cloud Services mit sich bringen. Das skizzierte Ausfallszenario hätte auch unabhängig davon, dass es einen Cloud Service betraf, auftreten können. Der Betreiber einer Datenbank in einem On-Premises-Data-Center hätte auch versehentlich den Abbau einer produktiven Datenbank veranlassen können.

Fehler passieren und werden auch zukünftig nicht zu vermeiden sein. Jedenfalls war der Cloud Service trotzdem so robust konzipiert, dass nach einiger Zeit wieder alles ohne Daten- und Funktionalitätsverlust hergestellt werden konnte. Abschließend die Nach- und die Vorteile im Überblick:

Nachteile

- Einige gute Ideen ließen sich wegen der eingeschränkten Funktionalität nicht umsetzen
- Gefühlte unsichere Handlungssituation in der „Lieferantenkette" aufgrund von fragiler Datenschutzlage (EU-U.S. Privacy Shield)
- Wenn etwas schiefgeht, hat man keinen Ansprechpartner im Haus und ist der Effektivität des Supports beim Cloud-Anbieter ausgeliefert

Vorteile

- 100-prozentige Entlastung im Betrieb
- Viel weniger ungeplante Ausfallzeiten
- Gewöhnung an die abgegebene Kontrolle und Genuss der Vorteile
- keine Lizenz- und Supportgebühren, sondern einfach ein monatlich kündbares Abonnement
- Skalierbarkeit lässt sich einfach online hinzukaufen
- Mehrere Oracle Cloud Services können von einem Ort aus verwaltet werden
- Die Erfüllung der immer höher und komplexer werdenden Datenschutzauflagen übernimmt der Cloud-Anbieter
- Know-how-Gewinn und Erhalt der eigenen Wettbewerbsfähigkeit
- Einschränkung in der Funktionalität des Schema Service hält die Anwendung technisch schlank und man konzentriert sich auf die fachliche Logik

Alexander Weber
alexander.weber@endlich.it