2022

Cloudbasierte Krankenhaus-IT

KONZEPTIERTE HANDLUNGSWEISE

OBERENDER AG | Elsenheimerstraße 59 | 80687 München

OBERENDER

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACM ..... *AWS Certificate Manager*
AWS KMS ..... *Key Management Service*
CD ..... *Continous Deployment*
CI ..... *Continous Integration*
CMK ..... *Customer Managed Key*
IAM ..... *Identity und Accessmanagement*
IPsec ..... *Internet Protocol Security*
KRITIS ..... *Kritische Infrastrukturen*
SSO ..... *Single Sign On*
TLS ..... *Transport Layer Security*
VPC ..... *Virtual Private Cloud*

Abbildungsverzeichnis

Executive Summary

Krankenhäuser müssen wirtschaftlich entlastet und zukunftsfähig aufgestellt werden. Um den neuen Anforderungen und der Komplexität im Bereich der IT gerecht zu werden, müssen die vorhandenen Personalressourcen zielgerichtet eingesetzt werden. Um diese Anforderungen zu erfüllen, wird hier ein Konzept zum Betreiben einer Cloud-Infrastruktur für Krankenhäuser vorgestellt. Der Begriff des Cloud-Computings orientiert sich in diesem Kontext dabei eng an den Definitionen des National Institute of Standards and Technology (NIST) aus September 2011[1].

- Eine Cloudlösung bietet den Anwendern besonders in kleinen Krankenhäusern eine **Entlastung** in vielen IT-Aufgaben sowie neue Services. Die sich daraus ergebende erhöhte Mitarbeiter-Produktivität resultiert aus dem in der Cloud realisierten Prinzip der zwischen Cloud-Anbieter und Kunden verteilten Verantwortlichkeit (**Shared Responsibility)** und ermöglicht dadurch eine erhöhte Agilität. Durch die so gewonnenen Freiräume lassen sich zum Bespiel die Herausforderungen und Aufgaben, die das Krankenhauszukunftsgesetz mit sich bringt, mit dem bestehenden Personalressourcen besser lösen.
- **Elastizität** und **Ressourcenpooling** ermöglichen den Krankenhäusern, den IT-Betrieb genau an ihre Anforderungen anzupassen. So sind das zeitweise Abschalten von Servern oder die dynamische Erhöhung von Rechenkapazitäten in Spitzenzeiten Merkmale einer Cloudlösung, die direkt Einfluss auf die Kostenstruktur des IT-Betriebes haben (Pay-as-you-go).
- Krankenhäuser arbeiten mit äußerst **sensiblen Daten**. Daher müssen höchstmögliche **Sicherheitsstandards** erfüllt werden. In einer Cloud-Lösung werden Daten durch **Verschlüsselungstechnologien** sowohl auf dem Transportweg wie auch in Ruhe (auf dem Speichermedium) verschlüsselt. Die Schlüssel befinden sich im Besitz des Krankenhauses
- Über all das gesagte hinaus ermöglicht eine Cloud-basierte Struktur mehr als die bloße virtualisierte Abbildung einer physikalischen IT-Infrastruktur. Neuartige Techniken zur Realisierung von Interoperabilitätsmodellen, Datenhaltung und -verwaltung sowie Formen des verteilten und mobilen Arbeitens sind nur einige der Potentiale einer Cloud-Lösung.

[1] Mell P, Grance T: The NIST Definition of Cloud Computing. https://doi.org/10.6028/NIST.SP.800-145 (Abgerufen: 12.04.2022)

Cloud Computing

Diverse Gründe für eine Migration in die Cloud

Die Krankenhäuser in Deutschland haben historisch aus vielen Gründen den Einsatz von Informationstechnologien sehr stiefmütterlich behandelt. Fehlende oder falsch allokierte finanzielle Mittel, wenig attraktive Arbeitsbedingungen für IT-Professionals und falsch verstandene Ziele und Aufgaben von IT-Dienstleistungen auf der Unternehmensleitungsebene sind nur einige Ursachen für die aktuelle Situation. Nur durch neue Denkrichtungen bezüglich der Unternehmensarchitektur und gleichzeitig durch die Entlastung der knapper personeller und finanzieller IT-Ressourcen kann unter diesen Umständen eine digitale Transformation des Gesundheitswesens gelingen.

Die besonders im Krankenhaus getätigten Investitionen in IT-Sicherheit der letzten Jahre haben das initiale Sicherheitsniveau eher reaktiv angehoben. Ausnahmen davon waren Krankenhäuser mit Einstufung als Kritische Infrastruktur (KRITIS-Einstufung), die hinsichtlich ihrer Systemrelevanz strenge Vorgaben zur IT- und Betriebssicherheit umsetzen mussten. Durch die jetzt für alle Krankenhäuser verpflichtende Einführung eines angemessenen Sicherheitsstandards (§75c Sozialgesetzbuch (SGB) V) sind gemanagte und messbare Richtlinien, die für alle wesentlichen Anlagen eingesetzt werden, der nächste Schritt. Das erhöht bei wünschenswerten Zielen nochmals die Anforderungen an Mitarbeiter, Management und die IT-Abteilungen der Krankenhäuser.

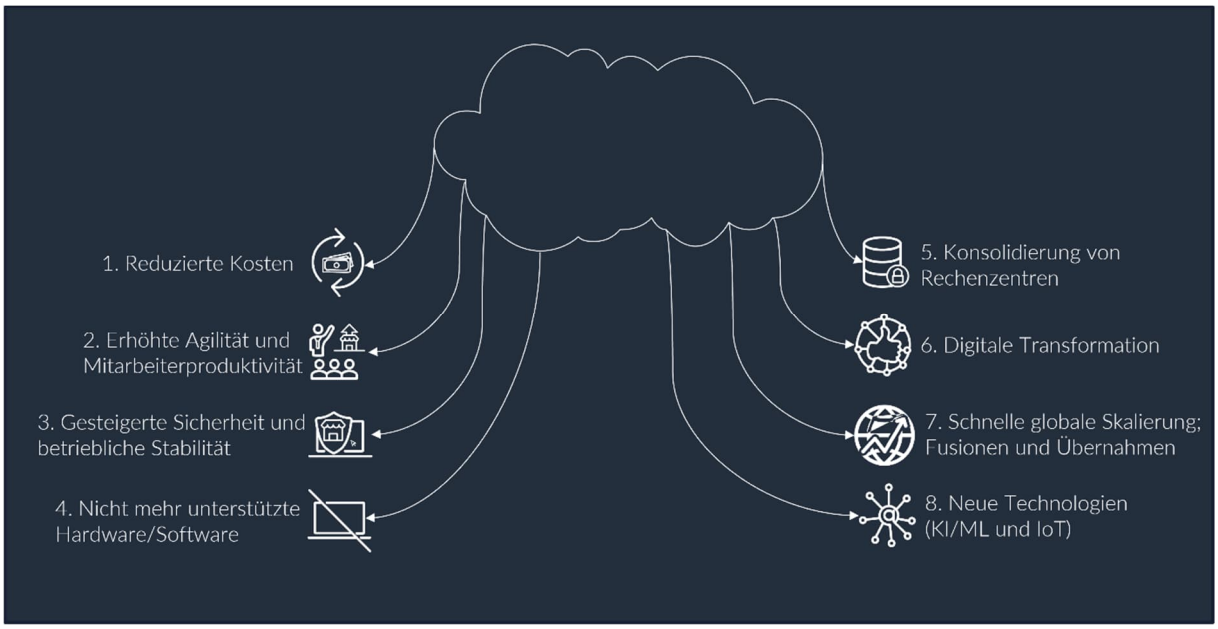

Abbildung 1: Geschäftsfaktoren für Migration zur Cloud, Anlehnung an AWS

Das vorliegende Konzept des cloudbasierten Krankenhauses liefert auf der Basis der vorherigen Ausführungen einen Lösungs-Baustein und erörtert die Voraussetzungen einer solchen Struktur unter Berücksichtigung der Tatsache, dass Krankenhäuser mit äußerst sensiblen Daten umgehen und daher höchstmögliche Sicherheitsstandards erfüllen müssen. Digitalisierung erfordert viele Änderungen und eine erhebliche Menge an weitreichenden Entscheidungen.

Mit der Cloud ist es möglich, Teams fortschrittliche Plattformen an die Hand geben und so deren Umsetzungskompetenz und -geschwindigkeit zu steigern.

Um den damit einhergehenden Risiken zu begegnen, werden im Rahmen dieses Konzeptes geeignete Methoden (Arbeitsweisen, Prozesse, Standards und akzeptierte Normen) aufgeführt. Hierbei ist es wichtig, nach der Erreichung eines Status quo im Rahmen eines Qualitätsmanagements, diese Methoden regelmäßig auf ihre Gültigkeit zu überprüfen.

In Ergänzung dazu können Ressourcen eingespart werden, indem Mechanismen etabliert werden, die automatisch die gesetzten Standards nachhalten. Instrumente hierfür werden von den Cloudplattformen bereitgestellt.

Sicherheit und Compliance

Als Teil der systemkritischen Infrastruktur sind Krankenhäuser für Angreifer besonders attraktive Ziele. Entsprechend wird die Abbildung des Sicherheitsaspektes im Krankenhauszukunftsgesetzt nicht nur im Fördertatbestand zehn, sondern auch anteilig in allen anderen Fördertatbeständen gefordert. Es ist nicht unwahrscheinlich, dass dies der Vorbereitung auf eine Zeit dient, in der, ähnlich wie im Bankensektor, die Betriebserlaubnis für ein Krankenhaus an die Erfüllung von IT-Sicherheitsstandards geknüpft wird. Im folgenden Kapitel werden die sieben Designprinzipien einer Cloud-Konzeption dargestellt und – so weit von einer konkreten Architektur unabhängig möglich – Lösungswege aufgezeigt.

Implementierung von Identity- und Accessmanagement (IAM)

Das erste Prinzip, um das höchstmögliche Maß an Sicherheit und Compliance zu erzielen, ist die sparsame Zuteilung von Berechtigungen. Es gilt: „So viel wie nötig, so wenig wie möglich“. Auf diese Weise wird eine Aufgabentrennung bereits durch die dafür notwendigen Berechtigungen erzwungen. Jeder Nutzer kann also nur diejenigen Aufgaben übernehmen, für deren Bearbeitung er im System die entsprechenden Berechtigungen hat. Die Zuteilung, Wartung und Verfolgung dieser Privilegien - Identitätsverwaltung genannt - sollten an einem Ort konzentriert werden. Dafür bietet sich z.B. Azure AD SSO (AD: Active Directory; SSO: Single-Sign-On) an.

Sicherstellung von Nachvollziehbarkeit

Ziel ist es, Aktionen und Änderungen an und in Ihrer Umgebung in Echtzeit zu überwachen, daraus entstehende Warnungen und Hinweise zu überprüfen und Gesamtprüfungen durchzuführen. Dies wird von allen Systemen ausführlich in Protokollen

dokumentiert. Da einige der Überwachungssysteme zu automatischen Untersuchungen in der Lage sind, ist eine Anpassung von Regeln an die bestehenden Geschäftsprozesse nötig.

Sicherheit auf allen Ebenen

Um Sicherheit auf allen Ebenen zu generieren, wird ein Defense-in-Depth-Ansatz (IT-Sicherheitsstrategie für Netzwerke) mit mehreren Sicherheitskontrollen angewendet. Dies gilt unter anderem für die folgenden Komponenten: Netzwerkrand, Virtual Private Cloud (VPC), Lastausgleich, alle Instanzen und Rechendienste, Betriebssysteme, Anwendungen und Code.

Automatisierung bewährter Sicherheitsverfahren

Automatisierte und softwarebasierte Sicherheitsmechanismen verbessern die Möglichkeit und Fähigkeit, den Betrieb sicher, schnell und kosteneffizient zu skalieren. Damit kann das Unternehmen auf sich ändernde Anforderungen flexibel reagieren. Das kann die schnelle Bereitstellung neuer Infrastruktur-Komponenten oder die Anpassung von Leistungsmerkmalen von Komponenten betreffen. Hierfür werden sichere Architekturen und Kontrollen als Code in versionsgesteuerten Vorlagen definiert und verwaltet

Der Schutz von Daten bei der Übertragung und in Ruhe

Der bestmögliche Schutz wird erreicht, indem Daten nach ihrem Schutzbedarf klassifiziert und entsprechend behandelt werden. Das kann sich auf Zugriffsrechte, erlaubte Speicherorte und sogar auf die Übertragbarkeit beziehen. Weiterhin werden Verfahren, wie die Verschlüsselung mit kundenverwalteten Schlüsseln (AWS Key Managed Service (KMS), Customer Managed Service (CMK)), Tokenisierung und Zugriffskontrolle angewendet, um durchgehend ein angemessenes Schutzniveau zu gewährleisten.

So viel wie notwendig - so wenig wie möglich

Ziel ist es, Mechanismen und Tools einzusetzen, die den direkten Zugriff auf Daten oder deren manuelle Verarbeitung regulieren, reduzieren bzw. komplett verhindern. Dadurch wird das Risiko einer falschen Handhabung, unbeabsichtigten Änderung oder Offenlegung besonders im Umgang mit sensiblen Daten verringert.

Etablierung eines Verfahrens für Sicherheitsvorfälle

Die Etablierung von Handlungsrichtlinien und Prozessen zur IT-Sicherheit ist notwendig, um im Falle eines Sicherheitsvorfalls, wie zum Beispiel eines Cyberangriffs, adäquat und umgehend reagieren zu können. Diese Handlungsrichtlinien sind mit den Anforderungen des Unternehmens abzugleichen. Sicherheitsvorfälle sollten in regelmäßigen Abständen unangekündigt simuliert und im Nachgang ausgewertet werden, um Routine des Teams im Umgang mit solchen Vorfällen zu schaffen. Automatisierte Tools erhöhen die Geschwindigkeit bei der Erkennung, Untersuchung und Wiederherstellung der Systeme.

Ende-zu-Ende Verschlüsselung

Im privaten Umfeld ist die Ende-zu-Ende-Verschlüsselung mittlerweile Standard. Bei einer korrekten Umsetzung können nur Sender und Empfänger die ausgetauschten Nachrichten lesen. Im Unternehmenskontext ist das Konzept vielerorts nicht umgesetzt. Das hängt auch mit einer konzeptionellen Denkweise über Vertrauen zwischen Kommunikationspartnern – seien es Menschen oder Maschinen – zusammen.

Bisher wurde davon ausgegangen, dass in einem kontrollierten (Unternehmens-)Netz das Vertrauen hinreichend durch die Mitgliedschaft im Netz definiert ist (Domänenrechner und Domänenbenutzer). Das war aber nie wirklich der Fall, da Angreifer von außen oder innen immer wieder durch Sicherheitslücken technischer oder organisatorischer Art eine Vertrauensstellung erlangen können, die ihnen weitreichende Rechte einräumen. Das gilt für „physikalische“ Netzwerke genauso wie für „virtuelle“ Netzwerke in der Cloud. Dem begegnet man mit dem Zero-Trust-Konzept.

Grundsätzlich wird keinem Gerät, keinem Anwender und keiner Anwendung vertraut. Zur Umsetzung dieses Konzeptes werden neben besonderen Authentifizierungsmechanismen Verschlüsselungsverfahren bei jeder Datenspeicherung (at-rest: im Ruhezustand) und Datenübertragung (in-transit: bei Übertragung) benutzt.

Verschlüsselung im Ruhezustand

Solange Daten von Nutzern oder (Programm-)Systemen nicht aktiv „angefasst“ werden, sind diese automatisch verschlüsselt. Das wird durch ein Regelwerk erzwungen und kann nicht umgangen werden. Die Nutzung von Daten setzt also einen Entschlüsselungsprozess voraus. Der Verschlüsselungsstatus sowie die Anforderung eines Entschlüsselungsvorganges lassen sich jederzeit überwachen.

Implementierung einer sicheren Schlüsselverwaltung

Für die Verschlüsselung sind private Schlüssel notwendig. Diese müssen sicher und mit strenger Zugriffskontrolle gespeichert werden, z. B. durch Verwendung eines Schlüsselverwaltungsdienstes wie AWS KMS. Solche Schlüsselverwaltungsdienste stellen eine zusätzliche Sicherheitsebene dar, indem sie durch eine sogenannte „Umschlagsverschlüsselung“ private Schlüssel in einer Art virtuellen Safe hinterlegen. Allgemein sollte die Verwendung verschiedener Schlüssel und die Zugriffskontrolle auf die Schlüssel in Kombination mit den AWS IAM- und Ressourcenrichtlinien erwogen werden, um die Datenklassifizierungsebenen und Trennungsanforderungen zu erfüllen.

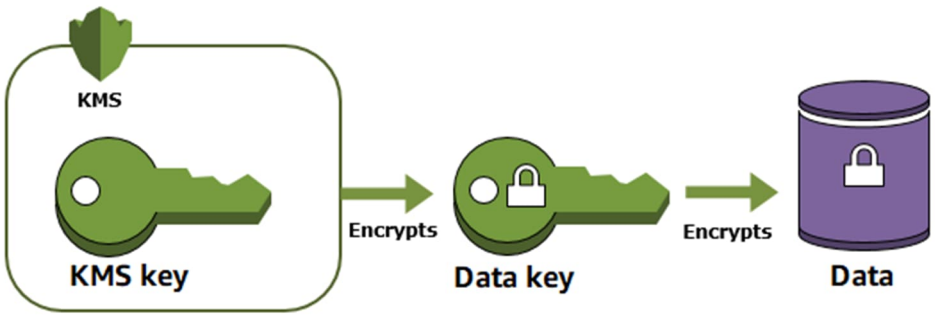

Abbildung 2: Beispielverschlüsselung mit AWS KMS mit CMK, Quelle: AWS

Durchsetzung der Zugriffskontrolle

Bei der Gestaltung der Zugriffskontrolle, also der Vergabe der Rechte und Mechanismen (einschließlich Backups, Versionierung und Isolierung) sollte so zurückhaltend wie möglich vorgegangen werden. An dieser Stelle sollte darüber hinaus kontrolliert werden, welche Daten öffentlich zugänglich sind.

Sicherstellung der personenspezifischen Zugriffe

Unter normalen Betriebsbedingungen sollte es den Benutzern eines Systems nicht möglich sein, direkt auf sensible Daten und Systeme zuzugreifen. Dies kann zum Beispiel realisiert werden, indem Benutzer nur über ein Dashboard Abfragen durchführen können, dabei jedoch keinen direkten Zugriff auf den Datenspeicher bekommen.

Wenn der Zugriff auf und die Funktionalität von einem System nicht durch die Anwendung von Continous-Integration- (CI) / Continous-Deployment (CD)-Pipelines sichergestellt wird, dann sollte ein Notfallaccount, auch „Break-Glass-Zugriffsmechanismus“ genannt, eingerichtet werden. Im Vergleich zu traditionellen Ansätzen werden diese Rechte nur im Ausnahmefall gewährt und es erfolgt eine Alarmierung und Prüfung.

Exkurs: CI/CD

„CI/CD“ beschreibt eine Methode, welche die regelmäßige Bereitstellung von Apps für Kunden umfasst und sämtliche Phasen der Anwendungsentwicklung automatisiert. Die Hauptkonzepte von CI/CD nennen sich „Continuous Integration “, „Continuous Delivery“ und „Continuous Deployment“. CI/CD löst Probleme auf, welche bei der Integration von neuem Code für Development-Operations (DevOps) -Teams entstehen können, beispielsweise im Zusammenhang mit der zeitlichen Realisierung von neuen Eigenschaften.

CI/CD sorgt speziell für eine kontinuierlich stattfindende Automatisierung und Überwachung über den gesamten Produktlebenszyklus einer App hinweg, beginnend bei der Integrations- und Testungs- und mündend in die Bereitstellungs- und Implementierungsphase. Diese zusammenhängende Kaskade wird demnach häufig als „CI/CD-Pipeline" beschrieben und wird durch eine enge Zusammenarbeit der DevOps-Teams umgesetzt.

Die schnelle Wiederherstellung von Anwendungen werden somit bei jedem Prozessdurchlauf ausgelöst. Dadurch können auch Veränderungen schnell rückgängig gemacht und etwaige Sicherheitsvorfälle schneller behoben werden.

Verschlüsselung bei Übertragung

Die Etablierung verschiedener Kontrollinstanzen ist obligat, um das Risiko unbefugter Zugriffe und Datenverluste im Zuge einer Datenübertragung zu minimieren.

Weiterhin ist es ratsam einen Zertifikatsverwaltungsdienstes, wie zum Beispiel den AWS Certificate Manager (ACM), zu verwenden, um eine sichere Verwaltung von Zugriffsschlüsseln und Zertifikaten zu ermöglichen und Datenzugriffe streng zu überwachen. Die Schlüssel und Zertifikate werden automatisch in regelmäßigen Abständen erneuert.

Erzwingen von Verschlüsselung bei der Übertragung

Organisatorische, rechtliche und Compliance-Anforderungen sind wesentliche Fokusthemen in Bezug auf die Datensicherheit in der Cloud. Hierfür sind Verschlüsselungsanforderungen und -verfahren zu definieren, welche auf Standards und aktuellen Empfehlungen basieren.

Automatisieren der Erkennung von unbeabsichtigtem Datenzugriff

Die Anwendung spezieller Erkennungs-Tools, wie beispielsweise AWS GuardDuty, ermöglicht es, Versuche von nicht autorisierten Datentransfers in nicht dafür vorgesehene Bereiche auf der Grundlage von Datenklassifizierungsstufen automatisch zu erkennen. Hierbei sind zum Beispiel Trojaner-Anwendungen identifizierbar, welche Daten anhand des Domain Name System (DNS)-Protokolls in ein nicht bekanntes bzw. nicht vertrauenswürdiges Netzwerk kopieren.

Authentifizierung der Netzwerkkommunikation

Die Überprüfung der Netzwerkkommunikation in Hinblick auf deren Identität sollte anhand von Protokollen erfolgen, welche die Authentifizierung unterstützen. Hierzu zählen z.B. Transport Layer Security (TLS) oder Internet Protocol Security (IPsec).

Zuverlässigkeit

Nachfolgend werden die fünf Grundsätze dargestellt, auf welchen die Zuverlässigkeit in der Cloud basiert.

Automatische Erkennung und Wiederherstellung nach Fehlern

Durch die Überwachung der für wichtige Leistungsindikatoren (idealerweise geschäftliche Indikatoren wie z.B. Anzahl an Labor- oder Röntgenuntersuchungen pro Stunde) erbrachte Rechenleistung, kann ein automatisierter Prozess angestoßen werden, wenn ein Grenzwert überschritten wurde. Das ermöglicht nicht nur die Benachrichtigung über und die Nachverfolgung von Fehlern, sondern auch das Anstoßen von Wiederherstellungsprozessen, die Fehler umgehen oder reparieren sollen. Dies kann bis zu dem Punkt vorangetrieben werden, an dem es möglich ist, Fehler zu antizipieren und zu beheben, bevor sie auftreten.

Testung von Wiederherstellungsverfahren

In einer On-Premise-Umgebung werden häufig Last-Tests durchgeführt, um nachzuweisen, dass die benötigte Rechenleistung in einem vordefinierten Szenario erbracht werden kann. Diese Testungen werden in der Regel nicht zur Validierung von Wiederherstellungsstrategien verwendet.

In der Cloud können Testumgebungen mit Hilfe von Continous Deployment (siehe Exkurs CI/CD) konsistent bereitgestellt und Wiederherstellungsverfahren so validiert werden.

Mithilfe der Automatisierung sind verschiedene Ausfälle simulierbar oder Szenarien nachstellbar, die zuvor zu Ausfällen geführt haben. Mit diesem Ansatz können Fehler-

pfade aufgedeckt werden, die getestet und behoben werden können, bevor ein reales Fehlerszenario eintritt. Insgesamt kommt es so zu einer Minimierung des Risikos.

Horizontale Skalierung erhöht Gesamtverfügbarkeit der Anwendung

Anstelle einer zentralen Instanz für alle Anfragen werden die Anfragen auf mehrere kleinere verteilt. Auf diese Weise werden die Auswirkungen eines einzelnen Ausfalls (vermeiden von Single Point of Failure) auf die Anwendung und somit Betriebsfähigkeit minimiert.

Die korrekte Planung/Reservierung von Kapazität

Eine häufige Ursache für Ausfälle bei lokalen Anwendungen ist ein unerwartet hohes Aufkommen an Anforderungen, die die Leistungsfähigkeit der bereitgestellten Ressourcen übersteigt. Dies ist häufig das Ziel von Denial-of-Service-Angriffen, d.h. durch eine Vielzahl von gezielten Anfragen verursachte, mutwillige Dienstblockade. In der Cloud können Sie die Nachfrage und die Auslastung der Anwendung überwachen und somit das Leistungsangebot an die Nachfrage anzupassen, ohne dass es zu einer Überlast oder Leerlauf kommt. Weiterhin sorgt dieses Procedere dafür, dass lediglich die Leistung bezahlt wird, die in Anspruch genommen wird (pay-as-you-go).

Änderungen durch Automatisierung

Änderungen an der Infrastruktur werden empfehlenswerter Weise mithilfe von automatisierten Prozessen (sogenannten Pipelines) vorgenommen. Diese Automatisierungsprozesse sind regelmäßig zu überwachen sowie zu überprüfen.

Operative Exzellenz

IT-Betrieb-as-Code leben

In einer Cloud ist die gesamte Umgebung „programmierbar“, so dass alle Anwendungen und die Infrastruktur als sogenannter Code definiert werden und upgedatet werden können. Auch (regelmäßig wiederkehrende) Betriebsaufgaben sind zum Beispiel so programmierbar, dass diese automatisch als Reaktion auf vordefinierte Ereignisse erfolgen können. Der IT-Betrieb via Code bringt den wesentlichen Vorteil mit sich, dass menschliche Fehler aufgrund der technischen Regelungen verringert werden und technische Fehler leichter reproduziert werden können. Dies erleichtert die Entwicklung zukünftiger Vermeidungsstrategien.

Änderungen sind häufig, klein und umkehrbar

Anpassungen von Komponenten sollten regelmäßig und in kurzen Zeitabständen möglich sein, so dass die daraus resultierenden Änderungen kleiner und leichter umkehrbar sind, sollte dies erforderlich werden. Idealerweise werden diese Änderungen so umgesetzt, dass sie den regulären Ablauf nicht beeinträchtigen.

Fehlerkultur etablieren

Für eine erfolgreiche Umsetzung des Cloudprojektes ist es bedeutsam, eine konstruktive Fehlerkultur unter den Mitwirkenden zu entwickeln. Diese wird durch einen regelmäßigen Austausch und ein Format, wie beispielsweise das „lessons learned“ erst tatsächlich gelebt.

Leistungseffizienz

Nachfolgend werden die vier Designprinzipien für die Leistungseffizienz in der Cloud dargestellt.

Demokratisierung fortschrittlicher Technologien

Es ist ratsam, komplexe Aufgabenteile an den Cloud-Anbieter abzugeben, um den Mitarbeitern den Prozess der Cloud-Implementierung und damit zusammenhängender Technologien zu erleichtern. So bietet es sich an, diese komplexen Aufgaben und Technologien, für deren Durchführung und Benutzung ein Spezialistenwissen erforderlich ist, als Software-Dienstleistung zu beziehen. Dazu zählen beispielsweise NoSQL-Datenbanken, Medientranskodierung und maschinelles Lernen. In der Cloud werden diese Technologien zu Services, welche die Mitarbeiter nutzen können. Zudem können sich dann die Mitarbeiter auf die Produktentwicklung konzentrieren, anstatt sich um die Bereitstellung und Verwaltung von Ressourcen zu kümmern.

Verwendung serverloser Architekturen

Serverlose Architekturen machen es für geeignete Anwendungen überflüssig, dass Server betrieben und gewartet werden müssen. So können beispielsweise serverlose Speicherdienste als statische Websites fungieren (wodurch Webserver überflüssig werden) und Ereignisdienste (Function as a Service) können ausführbaren Code (ohne Server) bereitstellen. Dadurch entfällt die operative Belastung durch die Verwaltung von Servern und die Kosten können gesenkt werden, da Clouddienste erheblich von Skaleneffekten profitieren.

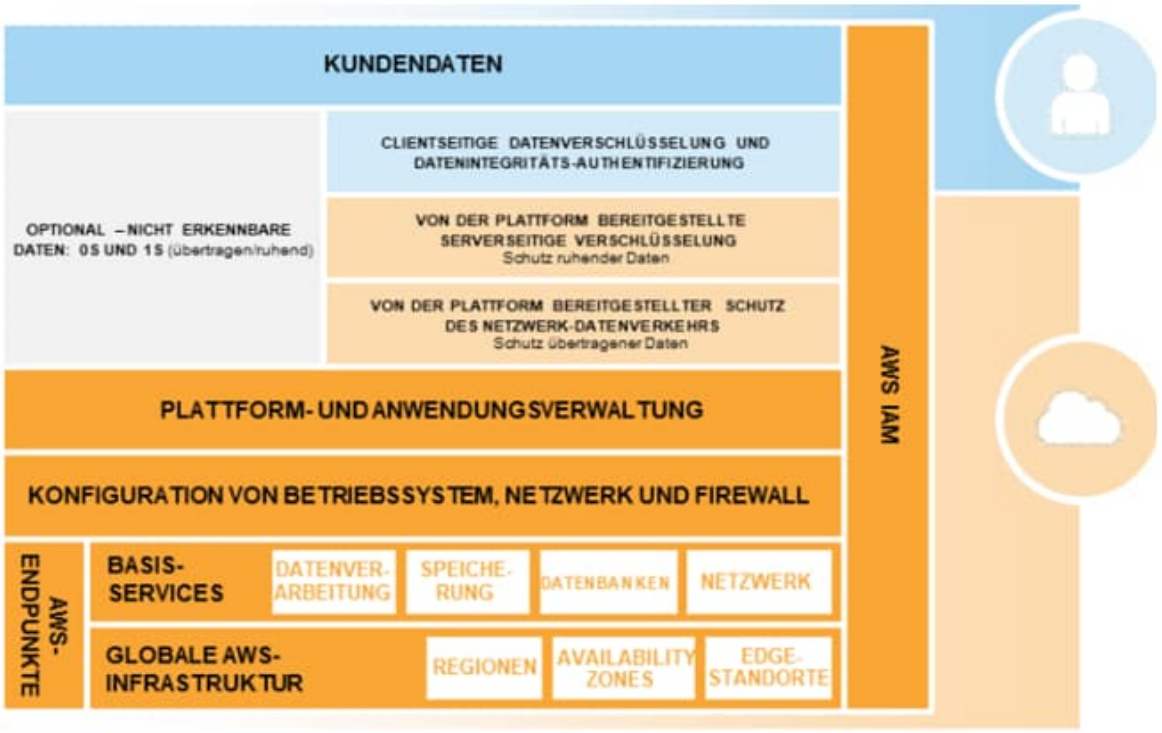

Abbildung 3: Das Modell geteilter Verantwortung für abstrakte Services; Quelle: AWS

Experimentierfreudigkeit

Die Etablierung einer Cloud bietet die Chance, eine passgenaue IT-Lösung für ein Unternehmen zu finden. Hierbei lohnt es sich experimentierfreudig zu sein und vergleichende Testungen verschiedener Arten von Instanzen, Konfigurations- und Speichermöglichkeiten durchzuführen.

"Mechanic Sympathy"

Grundsätzlich gilt es zu verstehen, wie Cloud-Dienste genutzt werden, um infolgedessen den technologischen Ansatz zu verwenden, der am besten mit den gesteckten Anwendungs-Zielen übereinstimmt. Werden Datenbank- oder Speicheransätze ausgewählt, sind Datenzugriffsmuster zu berücksichtigen.

Kostenoptimierung

Es sind verantwortliche Schlüsselfiguren zu definieren, welche für ein beständiges **Cost-Controlling** verantwortlich sind, um eine kontinuierliche Kostenoptimierung durchzuführen. Hierzu zählen vorzugsweise Mitarbeiter aus den Bereichen Finanzen und Controlling. Dabei sollten die folgenden Aspekte unbedingt beachtet werden.

Zusammenarbeit zwischen Finanzen und Technik

Beziehen Sie Ihre Finanzexperten in allen Phasen Ihrer Cloud-Journey in die geführten Diskussionen zu Kosten- und Nutzenabwägungen mit ein. In regelmäßigen Austausch-

gesprächen sollten die Verfolgung der Unternehmensziele, der aktuelle Stand der Kosten-Nutzen-Verhältnisse sowie Finanzberichte und die korrekte Verbuchung aller Sachverhalte Raum finden.

Cloud-Budgets und Prognosen

Die Berechnung sowie das Nachhalten und Anpassen eines cloudbezogenen Forecasts (Ist/Plan-Abgleich) sind dahingehend empfehlenswert, um auf Veränderungen der stark schwankenden Kosten und des Nutzens der Cloud reagieren zu können. Die Erfassungsprozesse sind dynamisch und trendbasiert zu gestalten, wobei im Idealfall situationsspezifische Algorithmen zur Anwendung kommen. Das Cost-Controlling sollte eine routinemäßige Tätigkeit darstellen, um Veränderungen umgehend proaktiv begegnen zu können. Die Zuordnung von Cloud-Ressourcen zu Kostenstellen ermöglich hier auch in Verbindung mit der Unternehmensbuchhaltung eine sachgerechte Zuordnung.

Kostenbewusstsein in organisatorischen Prozessen

Es ist von großer Bedeutung, die für das Projekt entscheidenden Schlüsselfiguren für die im Zuge des Projektes entstehenden Kosten zu sensibilisieren, um die erfolgreiche Umsetzung des Cloudprojektes sicherzustellen. Nur so lässt sich sicherstellen, dass das entstandene Kostenverständnis die Einhaltung des geplanten Budgets forciert. Auch Mitarbeiterschulungen sollten stets die entstehenden Kosten beleuchten.

Fort- und Weiterbildung im Bereich der Cloudlösungen

Es ist ratsam das kontinuierliche Gespräch mit Experten zu suchen, um innovative Dienste zeitnah nutzen zu können und um in Hinblick auf den Umgang mit der Cloudthematik stets auf dem neuesten Stand der Technik und Entwicklungen zu sein und die Effizienz des Unternehmens weiter zu steigern.

Relevanz im Kontext des Krankenhauszukunftsgesetzes

Bei den Fördertatbeständen des Krankenhauszukunftsgesetzes (KHZG), die erfüllt werden müssen, um die Förderungen bewilligt zu bekommen, nehmen die Vorgaben der Interoperabilität und IT-Sicherheit eine Schlüsselrolle ein. Es müssen mindestens 15 Prozent der für die Förderung eines jeweiligen Vorhabens beantragten Mittel für Maßnahmen zur Verbesserung der Informationssicherheit verwendet werden. Einen besonderen Fokus legt die Förderrichtlinie auf das Thema Interoperabilität. Als Beispiel lässt sich der Fördertatbestand 7 anführen, der das Thema Leistungsabstimmung und Cloud-Computing-Systeme definiert. Diesbezüglich sind Vorhaben nur dann förderfähig, wenn zur *„Herstellung einer durchgehenden einrichtungsinternen und einrichtungsexternen Interoperabilität digitaler Dienste auf international anerkannte technische, syntaktische und semantische Standards“* zurückgegriffen wird.[2]

Zusammenfassend: Keine Förderung durch das KHZG bekommt, wer die Vorgaben der Interoperabilität und IT-Sicherheit in seiner Digitalstrategie nicht berücksichtigt.

[2] Bundesamt für Soziale Sicherung: Richtlinie zur Förderung von Vorhaben zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhausaufenthaltes von Patientinnen und Patienten nach § 21 Absatz 2 KHSFV, https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Krankenhauszukunftsfonds/20210503Foerderrichtlinie_V03.pdf (Abgerufen: 07.04.2022)

Wirtschaftlichkeit

Die Vorteile und Konzepte rund um die Idee „Cloud-Betrieb“ erscheinen aus einer kaufmännischen Perspektive häufig abstrakt und übermäßig technisch. Dabei ist gerade die kaufmännische Rolle diejenige, die sich vehement für den Einsatz von Cloudtechnologie gegenüber einer On-Premise-Lösung einsetzen sollte:

Dazu eine Beispielrechnung anhand einer Infrastruktur für 300 virtuelle Desktops[3]:

Betriebskosten - Total Cost of Ownership (TCO) für einen Monat	**Virtual Desktop Infrastructure (VDI) Lösung**	
Kostenpunkt	**On-Premise**	**Cloud basierter Arbeitsplatz**
Hardware-Kosten		
Server Hardware für Compute-Hosts	€ 5.660	€ -
Server Hardware für Management-Hosts	€ 1.698	€ -
Server Hardware für Datenbank-Hosts	€ 2.312	€ -
Speicher Hardware	€ 7.298	€ -
Netzwerk Hardware	€ 1.934	€ -
Hardware-Pflege	€ 1.697	€ -
Energie und Kühlung	€ 4.026	€ -
Rechenzentrums-Speicher	€ 2.244	€ -
Software-Kosten		
Load Balancer/Access Gateways	€ 1.875	€ -
Virtual Desktop Software	€ 885	€ -
Client Access Lizenzen	€ 900	€ -
Administrations-Kosten		
Hardware Admin Kosten	€ 8.333	n/a
VDI Admin Kosten	€ 8.333	n/a
Desktop Management Admin Kosten	€ 8.333	€ 8.333
Cloud Ressourcen	€ -	€ 10.500
Summe	**€ 55.528**	**€ 18.833**
Einsparpotential gegenüber On-Premise		**66,08%**

[3] Amazon Web Services, https://aws.amazon.com/de/blogs/aws/tco-comparison-amazon-workspaces-and-traditional-virtual-desktop-infrastructure-vdi/ (Abgerufen: 08.04.2022)

Werden alle „versteckten“ Kosten inkludiert und eine transparente Vergleichsrechnung durchgeführt, erweist sich die Cloud-Lösung schon als die kostengünstigere Variante, in unserem Beispiel mit einem Einsparpotential von 66% gegenüber des On-Premise-Betriebs. Im dargestellten Rechenbeispiel werden dabei sogar viele Kostenfaktoren der On-Premise Lösung übergangen, wie beispielsweise unerwartete Reparaturen, steigende Energiekosten sowie die Herausforderung und der Ressourcenbedarf für Recruiting von IT-Fachpersonal.

Nachhaltigkeit

Optimierung für asynchrone und geplante Aufträge

Effiziente Software-Designs und passgenaue Architekturen sollen bewirken, dass der durchschnittliche Ressourcenbedarf je Arbeitseinheit grundsätzlich minimiert wird. Weiterhin ist es ratsam zusätzliche Mechanismen zu implementieren, die bewirken, dass alle Komponenten gleichmäßig ausgelastet werden sowie Leerläufe bei Ressourcen und Belastungsspitzen vermieden werden.

Entfernung oder Refactoring von Anwendungs-Komponenten

Eine Schlüsselmaßnahme sollte sein, Ressourcen so einzusetzen, dass keine ungenutzt bleiben. Hierfür sind die Workload-Aktivitäten zu überwachen, um Veränderungen in der Auslastung einzelner Komponenten im Laufe der Zeit zügig zu erkennen. Ungenutzte und nicht mehr benötigte Komponenten sollten entfernt und Komponenten mit geringer Auslastung (re-)implementiert werden. Folglich wird die Ressourcennutzung zielgerichtet minimiert und die Leistung gleichzeitig maximiert.

Auswirkungen auf Geräte und Infrastrukturen berücksichtigen

Bei allen Änderungen sollten die Auswirkungen auf Endgeräte und Infrastruktur berücksichtigt werden. Dabei sind der voraussichtliche Lebenszyklus (Abschreibung, Leasing etc.) und die notwendigen Investitionen zu berücksichtigen. Es sollten Software und IT-Architekturen verwende werden, die möglichst keine Notwendigkeit für einen vorzeitigen Austausch erzeugen. Auch Hardware und Betriebssystemkompatibilitäten sind zu berücksichtigen und der Ressourceneinsatz auf den Zustand der Endgeräte, in Hinblick auf Leistungsfähigkeit und Speicherkapazität, abzustimmen.

Verwendung geeigneter Speicherdienste

Für die Wahl der Technologien zur Minimierung von Datenverarbeitungs- und Speicheranforderungen gilt es zunächst nachzuvollziehen, wie Daten innerhalb des Ökosystems verwendet werden. Deshalb ist eine Betrachtung des Datenkonsums sowie des Prozesses der Übertragung und Speicherung von Daten notwendig.

Cloud-Konzept der Oberender AG

Für die erfolgreiche Migration in die Cloudbasierte Krankenhaus-IT ist ein breites Spektrum an Know-how und Expertise erforderlich. Aufgrund der Ressourcenknappheit im Bereich des IT-Personals und der Liquidität sowie der Komplexität sind Kliniken auf Unterstützung in der Realisierung derartiger Projekte angewiesen. Oberender AG bietet die Planung und Umsetzung eines passgenaues Cloud-Konzepts für Krankenhäuser an. Durch die Abbildung aller relevanten Funktionalitäten und eine Potenzialanalyse kann die Migration individuell und ressourcenschonend geplant und umgesetzt werden.

Sprechen Sie uns an:

Oberender AG
Kompetenzteam Digitalisierung und Medizincontrolling
Elsenheimerstr. 59
80687 München
Tel: +49 89 8207516-0