Otto-von-Guericke Universität Magdeburg

IT-Notfallmanagement in der Cloud

Erfüllt ein cloudbasiertes IT-Notfallmanagement die Voraussetzungen, um redundante Notfallrechenzentren abzulösen?

Bachelorarbeit

Arbeitsgruppe Managementinformationssysteme

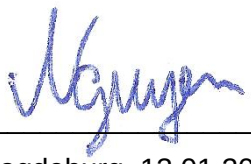
Betreuer: Prof. Dr. Hans-Knud Arndt

Vorgelegt von: Tuan Minh Nguyen

Abgabetermin: 13.01.2020

Selbstständigkeitserklärung

Hiermit erkläre ich, Tuan Minh Nguyen, dass ich die vorliegende Bachelorarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Ausführungen, die fremden Quellen, einschließlich Internetquellen, wörtlich oder sinngemäß entnommen wurden, sind als solche kenntlich gemacht worden. Dasselbe gilt für Tabellen und Abbildungen.



Magdeburg, 13.01.2020

Inhaltsverzeichnis

Abkürzungsverzeichnis

BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
BIA	Business Impact Analyse
DR	Disaster Recovery
HA	High Availability
NIST	National Institute of Standards and Technology
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RZ	Rechenzentrum
VM	Virtuelle Maschine

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1 Problemstellung

Heutzutage durchdringt die Digitalisierung nahezu alle Tätigkeiten des Alltags, sodass es selbstverständlich erscheint stets ununterbrochenen Zugang zu sozialen Medien, Nachrichtenseiten oder das E-Mail-Postfach zu haben. Besonders bekannte Dienste scheinen nie oder nur sehr selten nicht verfügbar zu sein. Um diese Ausfallsicherheit zu gewährleisten sichern Organisationen die IT-Infrastruktur hinter diesen Diensten ab.

Fast jedes Unternehmen betreibt eigene IT-Systeme, die oft mit dem Betrieb eigener Rechenzentren verbunden sind.[1] Da die IT für die meisten Geschäftsprozesse unabdingbar geworden ist, gilt es ihren Betrieb sicherzustellen und ihre Infrastruktur vor Ausfällen zu schützen. Gefahren für den Betrieb der IT-Infrastruktur können Cyberangriffe, natürliche Katastrophen aber auch terroristische Angriffe sein. Eine traditionelle Lösung das Risiko bzw. die Dauer eines IT-Ausfalls zu verringern ist es eine redundante IT-Infrastruktur bereitzustellen. Sollte der Notfall eintreten und die primäre IT-Infrastruktur ausfallen, so kann auf diese Notfallsysteme geschwenkt werden. Im Idealfall kriegen die Benutzer außer einer kleinen Verzögerung, vom Ausfall bis zum vollendeten Failover, dem Schwenk auf die Notfallsysteme, nichts von diesem Prozess mit.[2] Diese Lösung hat sich bisher bewiesen und stellt heute die dominierende Strategie dar lange IT-Ausfälle zu vermeiden.

In letzter Zeit steht durch den Vormarsch des Cloud Computing jedoch eine neue Möglichkeit im Raum, die IT von Unternehmen und Organisationen zu schützen. Nach einem Ausfall des primären Rechenzentrums soll, anstatt auf ein zweites redundantes Notfall-Rechenzentrum, zu Notfallsystemen in einer Cloud geschwenkt werden. Durch diese kann auf die kostenintensive Bereitstellung und Wartung eigener Systeme verzichtet werden. Der Cloud-Dienstleister ist für die IT-Ressourcen verantwortlich und stellt sie dem Kunden zur Zeit des Notfalls zur Verfügung.

1.2 Zielsetzung

Die Untersuchung in dieser Arbeit soll zeigen ob ein cloudbasiertes Notfallmanagement in der Lage ist, redundante Notfallrechenzentren abzulösen. Um dies bestimmen zu können werden beide Arten des Notfallmanagements analysiert und anhand ausgewählter Untersuchungsgegenstände miteinander verglichen. Es besteht bei Nutzung der Cloud-

[1] Vgl. Hintermann und Clausen 2014.

[2] Vgl. Brotherton und Dietz 2014, S. 2.

Technologie zwar die Möglichkeit, die gesamte IT-Infrastruktur mitsamt primären Systemen in die Cloud auszulagern, in dieser Arbeit wird aber nur die Verlagerung im Notfall untersucht.

1.3 Inhaltliche Gliederung

In Kapitel 2 *Theoretische Grundlagen* wird grundlegendes Wissen zu Notfallmanagement, Cloud und IT-Infrastruktur vermittelt werden. Zu Beginn des Kapitels wird die zu schützende IT-Infrastruktur mit den zu ihr gehörenden Komponenten erklärt. Danach folgt eine Einführung in das Cloud Computing mit einer Vorstellung der verschiedenen *Service-* und *Nutzungsmodelle*. Am Ende des Kapitels wird das Thema Notfallmanagement näher beleuchtet. Hier wird zudem erläutert was unter traditionellem und cloudbasiertem Notfallmanagement zu verstehen ist.
In Kapitel 3 *Untersuchungsgegenstände* werden fünf Aspekte untersucht, anhand derer das traditionelle mit dem cloudbasierten Notfallmanagement verglichen wird.
Abschließend folgt in Kapitel 4 das *Resümee*, in dem die Erkenntnisse aus der Arbeit zusammengefasst werden.

2. Theoretische Grundlagen

In diesem Kapitel wird zunächst grundlegendes Wissen zu IT-Infrastrukturen mit Erklärungen zu den Komponenten vermittelt, die eine IT-Infrastruktur ausmachen. Danach folgt eine Einleitung zum Cloud Computing mit Erklärungen zu Service- und Nutzungsmodellen. Zum Ende des Kapitels wird das Thema Notfallmanagement mit den beiden zu untersuchenden Varianten, traditionelles und cloudbasiertes Notfallmanagement, vorgestellt.

2.1 IT-Infrastruktur

Im Alltag wird der Begriff *Infrastruktur* oft mit Straßen, Schienen oder auch Stromnetzen assoziiert. Alle drei sind notwendige Komponenten einer Volkswirtschaft, ohne die eine Güterproduktion im selben Maße nicht möglich wäre. Wie die allgemeine Infrastruktur für eine Volkswirtschaft, so ist eine IT-Infrastruktur für die Leistungserstellung mit Informationstechnik unverzichtbar. Der Ausfall einer kritischen Komponente der IT-Infrastruktur kann sich negativ auf den Geschäftsbetrieb auswirken. Aus diesem Grund ist der Schutz der IT-Infrastruktur im Fokus eines funktionierenden Notfallmanagement.[3]

Die IT-Infrastruktur wird zwar je nach Quelle leicht unterschiedlich definiert, jedoch besteht Einigkeit darin, dass sie die für den Betrieb von (Anwendungs-)Software notwendigen Komponenten beinhaltet. Während der Begriff nach einigen Ansätzen nur technische Komponenten umfasst, wird er von anderen um organisatorische Strukturen und Prozesse erweitert.[4] Im Folgenden dieser Arbeit orientiert sich Nutzung des Begriffs an der Definition von Laudon. Nach Laudon et al. setzt sich eine IT-Infrastruktur aus den folgenden sieben Hauptkomponenten zusammen:[5]

Datenmanagement und -speicherung: Physikalische Datenspeicher und Datenbankmanagementsysteme werden benötigt, um Daten unternehmensweit zur Verfügung zu stellen. Heutzutage werden die Speicher oft als Netzwerk, auch Storage Area Network (SAN) genannt, miteinander verbunden.

Internetplattformen: Unter Internet als Plattform werden die Komponenten (Dienste, Hard- und Software) verstanden, die für den Betrieb der Webdienste der Organisation verantwortlich sind.

[3] Vgl. Watters 2014, S. 9.

[4] Vgl. Rudolph 2009, S. 30–31.

[5] Vgl. Laudon et al. 2016, S. 215.

Hardwareplattformen: Mit IT-Infrastruktur Hardwareplattformen sind hierbei Client- und Servermaschinen gemeint. Clients wie Desktop-PCs oder Laptops stellen die Geräte der Anwender dar. Server sind hierbei Maschinen, die Clients miteinander verbinden und diesen Rechenleistung zur Verfügung stellen können.

Betriebssystemplattformen: Betriebssysteme bilden die Schnittstelle zwischen den Hardware-Komponenten und der darauf betriebenen Software. Sie verwalten unter anderem die Nutzung und Auslastung der Hardware.

Betriebliche Anwendungssysteme (inkl. Middleware): Systeme, mit denen Aktivitäten, Entscheidungen und Kenntnisse über viele verschiedene Funktionen, Ebenen und Geschäftseinheiten hinweg in einem Unternehmen koordiniert werden können. Hierzu gehören Enterprise-Resource-Planning-, Supply-Chain-Management-, Kundenbeziehungs- und Wissensmanagementsysteme sowie Systeme für die (Gruppen-)Zusammenarbeit.[6]

Netzwerke / Telekommunikation: Netzwerke ermöglichen die unternehmensinterne Kommunikation und die Verbindungen zwischen Clients mit Servern. Die Telekommunikation umfasst Internetanbindungen sowie Telefondienste.

Unternehmensberatungen und Systemintegratoren: Die Wartung- und Weiterentwicklung von IT-Infrastrukturen wird meist von externen Dienstleistern durchgeführt. Unternehmen und anderen Organisationen fehlen oft die Kapazitäten sowie Expertise um, zum Beispiel die komplexe Einführung einer neuen Infrastruktur allein durchzuführen.

2.2 Cloud Computing

Ziel dieser Arbeit ist es, das traditionelle Notfallmanagement mit einem cloudbasierten zu vergleichen. Was aber zeichnet eine Cloud aus? Das *National Institute of Standards and Technology (NIST)*, eine Bundesbehörde für Standards der USA, definiert Cloud Computing als ein Modell für einen allgegenwärtigen, praktischen und je nach Nachfrage bereitgestellten Netzwerkzugriff auf gemeinsam genutzte konfigurierbare IT-Ressourcen. Mit Ressourcen sind hierbei als Beispiele Netzwerke, Server, Speicher, Anwendungen und Dienstleistungen genannt. Eine weitere Eigenschaft ist eine schnelle, sowie mit minimalen Management- oder Dienstleistungsaufwand verbundene Bereitstellung dieser Ressourcen.[7] Baun et al.

[6] Vgl. Laudon et al. 2016, S. 444.

[7] Vgl. Mell und Grance 2011.

schreiben, dass es keine standardisierte oder einheitliche Definition des Cloud Computing Begriffs gibt. Trotz dessen beschreiben sie Cloud Computing, ähnlich der NIST Definition, als Bereitstellung und Nutzung von IT-Infrastruktur, Plattformen und Anwendungen aller Art als im Internet elektronisch verfügbare Dienste.[8]

Für Organisationen ergeben sich mehrere Vorteile bei Nutzung von Cloud Computing. Aus wirtschaftlicher Sicht senkt eine Cloud deswegen Investitionskosten für neue als auch bereits bestehende Unternehmen. Bereitstellung und Wartung können von einem Dienstleister übernommen werden, dessen Dienste nach tatsächlicher Nutzung vergütet werden können. Einmalige hohe Fixkosten, beispielsweise für den Kauf sowie dem Aufbau der IT-Infrastruktur, entfallen somit.[9]

Im Zusammenhang mit Cloud Computing und genereller, ausgelagerten IT-Ressourcen, werden in der Literatur häufig die beiden Begriffe *On-Premise* und *Off-Premise* genannt. On-Premise bedeutet, dass Systeme innerhalb der eigenen IT betrieben werden, während Off-Premise Systeme bezeichnet, die von einem Dienstleister außerhalb der eigenen Organisation betrieben werden.[10]

2.2.1 Servicemodelle

Mithilfe einer Cloud können mitunter Anwendungen, Plattformen oder auch IT-Infrastrukturen als Dienstleistung zur Verfügung gestellt werden. Das NIST und viele andere Autoren unterteilen Cloud Angebote deswegen in folgende drei Servicemodelle, auch Cloud Service Delivery Models genannt.[11] [12]

Software as a Service (SaaS)

Der Dienstleister stellt seinen Kunden Anwendungssoftware in seiner Cloud Umgebung zur Verfügung. Beispiele hierfür sind Mailanwendungen oder Office-Anwendungen, die über das Internet bereitgestellt werden. Kunden sind reine Anwender und haben keine Administrationsmöglichkeit über die Software und die dahinterliegende Hardware. Der Zugriff erfolgt entweder über einen Webbrowser oder über eine Programmschnittstelle.[13] Auf eine

[8] Vgl. Baun et al. 2011, S. 1.

[9] Vgl. Marston et al. 2011, S. 178.

[10] Vgl. Kohne 2018, S. 26–27.

[11] Vgl. Mell und Grance 2011.

[12] Vgl. Subashini und Kavitha 2011, S. 3.

[13] Vgl. Mell und Grance 2011.

lokale Installation auf den Endgeräten der Nutzer kann damit verzichtet werden.[14] SaaS benötigt aus diesem Grund hauptsächlich eine ausreichende Internetverbindung zu den Servern des Dienstleisters. On-Premise werden somit weder nennenswerte Rechenleistung noch Speicherplatz benötigt.

Platform as a Service (PaaS)

Dem Kunden wird vom Cloud-Dienstleister eine Softwareentwicklungsplattform gestellt, auf welcher er, mithilfe vom Dienstleister gestellten Entwicklerwerkzeugen, seine eigenen oder von Drittanbietern entwickelte Anwendungen ausführen lassen kann. Die Verwaltung der dahinterliegenden Hardware und Infrastruktur obliegt auch hier dem Cloud-Dienstleister.[15] Als Beispiele für PaaS können die *Google App Engine* oder *Openshift* genannt werden.[16]

Infrastructure as a Service (IaaS)

Infrastructure as a Service umfasst den Zugriff auf eine virtualisierte IT-Infrastruktur die vom Cloudanbieter bereitgestellt wird.[17] Nutzer erhalten damit eine abstrahierte Sicht auf Hardware wie Rechner, Massenspeicher oder Netzwerke.[18] Anbieter von IaaS sind beispielsweise Microsoft oder Amazon Web Services.[19] Der Kunde kann auf der virtualisierten Hardware beliebige Betriebssysteme und sonstige Software installieren. IaaS bietet damit eine höhere Kontrolle über die IT-Ressourcen und kann auch, sofern gewünscht, die beiden anderen Servicemodelle SaaS und PaaS realisieren.[20]

2.2.2 Nutzungsmodelle

Im Grunde ist Cloud Computing eine Outsourcing-Dienstleistung zur Bereitstellung von IT-Ressourcen. Die Gestaltung dieser Bereitstellung kann jedoch sehr unterschiedlich erfolgen. Meist wird zwischen drei Bereitstellungsvarianten, den sogenannten Nutzungsmodellen, unterschieden. Namentlich sind dies Public, Private und Hybrid Cloud.[21] [22] [23] Einige Autoren in

[14] Vgl. Baun et al. 2011, S. 36.

[15] Vgl. Mell und Grance 2011.

[16] Vgl. Hossny et al. 2013, S. 2.

[17] Vgl. Mell und Grance 2011.

[18] Vgl. Baun et al. 2011, S. 30–31.

[19] Vgl. Gandhi und Kumbharana 2018, S. 121.

[20] Vgl. Bedner 2013, S. 29.

[21] Vgl. Münzl et al. 2015, S. 12.

[22] Baun et al. 2011, S. 26.

[23] Vgl. Stanoevska-Slabeva 2010, S. 59–62.

der Wissenschaft nennen zusätzlich zu den drei primären Nutzungsmodellen noch weitere wie die Community Cloud.[24]

Public Cloud

Heutzutage wird im Zusammenhang mit Cloud Computing oft von einer Public Cloud ausgegangen.[25] Eine Public Cloud wird von einem externen, nicht zur nutzenden Organisation gehörendem, Dienstleister betrieben. Der Dienstleister stellt die Cloud-Ressourcen einem nicht eingeschränkten Nutzerkreis zur Verfügung, d. h. mehrere Kunden können sich dieselben Ressourcen teilen. Die Verbindung zu einer Public Cloud erfolgt fast ausschließlich über das Internet. Bekannte Betreiber solcher Clouds sind Amazon Webservices, Microsoft Azure oder auch IBM.[26] [27]

Private Cloud

Private Clouds werden anstelle von einem externen Dienstleister, von der nutzenden Organisation selbst betrieben und verwaltet. Ein wichtiger Grund eine Private Cloud in Betracht zu ziehen ist die erhöhte Sicherheit gegenüber einer Public Cloud. Daten bleiben innerhalb der nutzenden Organisation und werden nicht auf fremden Servern gespeichert.[28] Unternehmensfremden wird damit der unbefugte Zugriff erschwert. Es werden zwar mehrere Nachteile einer Public Cloud vermieden, jedoch erreicht eine Private Cloud nicht dieselbe Kosteneffizienz, da trotzdem eigene Hardware beschaffen und betrieben werden muss.[29]

Hybrid Cloud

Die beiden bereits vorgestellten Modelle haben jeweils ihre Vor- und Nachteile. Eine Public Cloud ist zwar kosteneffizienter, bringt jedoch den Nachteil mit sich, das Daten auf organisationfremden Systemen gespeichert werden. Dies kann eine Reduktion der Datensicherheit bedeuten, da sich die nutzende Organisation auf die bereitstellende Organisation verlassen muss. Bei der Private Cloud verhält es sich genau gegenteilig. Die Idee bei einer sogenannten Hybrid Cloud ist es eine Kombination aus beider Nutzungsmodelle zu implementieren. Eine Hybrid Cloud, wie in Abbildung 1zu sehen, mindestens aus einer Private und einer Public Cloud, welche gemeinsam die IT-Prozesse der Organisation bereitstellen. Kerngeschäftsprozesse mit kritischen Daten werden On-Premise in einer Private

[24] Vgl. Bedner 2013, S. 36.

[25] Vgl. Münzl et al. 2015, S. 14.

[26] Vgl. Stanoevska-Slabeva 2010, S. 59–60.

[27] Vgl. Baun et al. 2011, S. 27–28.

[28] Vgl. Baun et al. 2011, S. 27–28.

[29] Vgl. Münzl et al. 2015, S. 14.

Cloud durchgeführt. Nichtkritische Prozesse können in eine Public Cloud ausgelagert werden.[30] [31]

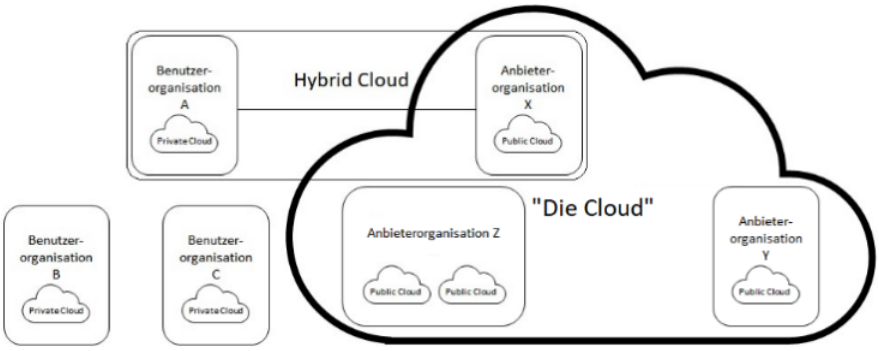


Abbildung 1: Cloud Servicemodelle[32]

Community Cloud

Eine Cloud-Infrastruktur, die mehrere ausgewählte Organisationen gemeinsam nutzen, wird Community Cloud genannt. Die Organisationen haben meist ähnliche Anforderungen bei Themen wie Sicherheit oder Compliance. Anders als eine Public Cloud steht die Community Cloud nur einer begrenzten Zahl von Organisationen zur Verfügung. Sie kann von einer oder mehreren der nutzenden Organisationen oder auch von Drittdienstleistern betrieben werden.[33] [34] [35]

[30] Vgl. Dillon et al. 2010, S. 28.

[31] Vgl. Lenk 2014, S. 47–48.

[32] Vgl. Baun et al. 2011, S. 27.

[33] Vgl. Dillon et al. 2010, S. 28.

[34] Vgl. Mell und Grance 2011.

[35] Vgl. Lenk 2014, S. 57.

2.3 IT-Notfallmanagement

2.3.1 Allgemein

Das IT-Notfallmanagement ist, nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI), ein komplexer Prozess und umfasst die Notfallvorsorge, die Notfallbewältigung sowie die Notfallnachsorge. Es verfolgt das Ziel einen funktionierenden Geschäftsbetrieb zu gewährleisten und Beeinträchtigungen durch Notfälle zu minimieren. Notfälle sind laut BSI Schadensereignisse, bei denen Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Sie unterscheiden sich von anderen Schadensereignissen wie Störungen, Krisen und Katastrophen durch den Grad der Geschäftsbetriebsbeeinträchtigung. Tabelle 1 zeigt eine vergleichende Übersicht über die verschiedenen Schadensereignisse.[36]

Tabelle 1: Klassifizierung von Schadensereignissen

Vorfall	**Erläuterung**	**Behandlung**
Störung	Prozesse oder Ressourcen einer Institution funktionieren nicht wie vorgesehen. Resultierende Schäden sind gering.	Störungen können durch im Tagesgeschäft integrierte Störungsbehebung behoben werden.
Notfall	Prozesse oder Ressourcen einer Institution funktionieren nicht wie vorgesehen. Verfügbarkeit dieser kann nicht innerhalb gefordert Zeit wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt und es entstehen hohe bis sehr hohe Schäden.	Die Behebung von Notfällen erfordert eine gesonderte Notfallbewältigungsorganisation.
Krise	Auf die Institution begrenzter verschärfter Notfall. Eine Krise gefährdet die Existenz der	Krisen können trotz vorbeugender Maßnahmen nicht von normaler Aufbau- und Ablauforganisation

[36] Vgl. Bundesamt für Sicherheit in der Informationstechnik 2008.

	Institution oder das Leben und die Gesundheit von Personen. Krisen stellen einmalige Ereignisse dar.	bewältigt werden. Die Verantwortlichkeit für die Behebung liegt beim internen Krisenmanagement.
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis. Für die einzelnen Institutionen stellt sich eine Katastrophe als Krise dar.	Katastrophen können durch deren großflächige Auswirkungen nicht mehr durch die Institution selbst behoben werden. Es bedarf der Hilfe des Katastrophenschutzes.

Business Continuity Management & Disaster Recovery

Im englischsprachigen Gebrauch und teilweise auch im Deutschen haben sich, im Zusammenhang mit Notfallmanagement, die beiden Begriffe *Business Continuity Management* (BCM) sowie *Disaster Recovery* (DR) etabliert. BCM ist ein Managementprozess und entspricht dem ganzheitlichen Notfallmanagementbegriff von der Vor- bis zur Nachsorge[37]. Mit Notfällen sind beim BCM Schadensereignisse gemeint, die mit einem Ausfall von Systemen oder einer Leistungsminderung einhergehen. Da die Definition eines IT-Notfallmanagements nach BSI Standard 100-4 ähnlich der von BCM ist werden beide Begriffe in dieser Arbeit synonym verwendet.

DR umfasst im Gegensatz zu den beiden anderen Begriffen lediglich die Wiederherstellung des normalen Betriebs ausgefallener IT-Systeme. BCM entwickelte sich mit der Zeit aus DR heraus, da bei Notfällen eine Beschränkung auf die Wiederherstellung der IT-Systeme nicht mehr ausreichte. Laut Erb wurde die Notwendigkeit nach umfassenderer Notfallplanung mitunter infolge von Terroranschlägen erkannt. Unternehmen erweiterten durch die zunehmende Abhängigkeit ganzer Geschäftsprozesse von der IT, ihre Notfallplanung um nicht IT-relevante Faktoren[38].

Business Impact Analyse

[37] Vgl. Kersten und Klett 2017, S. 64.

[38] Vgl. Erb 2015, S. 15–16.

Essenziell wichtig für den Notfallmanagementprozess ist eine Analyse der Auswirkungen, die ein Ausfall eines Geschäftsprozesses auf den Geschäftsbetrieb hätte. Diese wird allgemein Business Impact Analyse (BIA) genannt.[39] Infolge der BIA wird die Kritikalität jedes Geschäftsprozesses bewertet, woraus wiederum der Schutzbedarf ermittelt werden kann. Mit Kritikalität ist hierbei die Zeitkritikalität (siehe RPO / RTO) für den Wiederanlauf der Prozesse, nicht unbedingt die Wichtigkeit dieser für die Organisation, gemeint.[40]

Recovery Point Objective (RPO) & Recovery Time Objective (RTO)

Um ein effektives Notfallmanagement zu gestalten, muss definiert werden wann es überhaupt als solches gilt. Zu diesem Zweck gibt es zwei Messgrößen welche die zeitlichen Anforderungen an das Notfallmanagement, insbesondere Disaster Recovery, festlegen. Die *Recovery Point Objective* (RPO) legt fest wie lange die letzte Datensicherung zum Eintreten des Notfalls zurückliegen darf. Die *Recovery Time Objective* (RTO) gibt an wann kritische ausgefallenen Prozesse spätestens wiederaufgenommen werden müssen, bevor der Organisation ein größerer Schaden entsteht.[41] Da sich beide Messgrößen aus den individuellen Geschäftsanforderungen von Organisationen ableiten, können diese je nach Anwendungsfall sehr unterschiedlich bemessen sein.[42]

In Abbildung 2 ist der Ablauf einer DR-Wiederherstellung dargestellt, mit der RPO zeitlich vor und der RTO zeitlich nach Eintritt eines Notfalls. Die letzte Datensicherung sollte maximal die Zeitspanne der RPO erreichen, diese jedoch nicht überschreiten. Für die RTO ist es ausreichend, wenn bis innerhalb der Zeitspanne ein Notbetrieb mit ausreichend hoher Kapazität hergestellt werden kann.[43] Nach einer Rückführung vom Not- in den Normalbetrieb wird damit gerechnet, dass Nacharbeiten durchzuführen sind und die Kapazität des Betriebs deshalb kurzzeitig über der des Normalbetriebs steigt.[44]

[39] Vgl. International Organization for Standardization 2012.

[40] Vgl. Osterhage 2016, S. 66.

[41] Vgl. International Organization for Standardization 2011.

[42] Vgl. Andrade et al. 2017, S. 948.

[43] Vgl. Osterhage 2016, S. 17–18.

[44] Vgl. Bundesamt für Sicherheit in der Informationstechnik 2008.

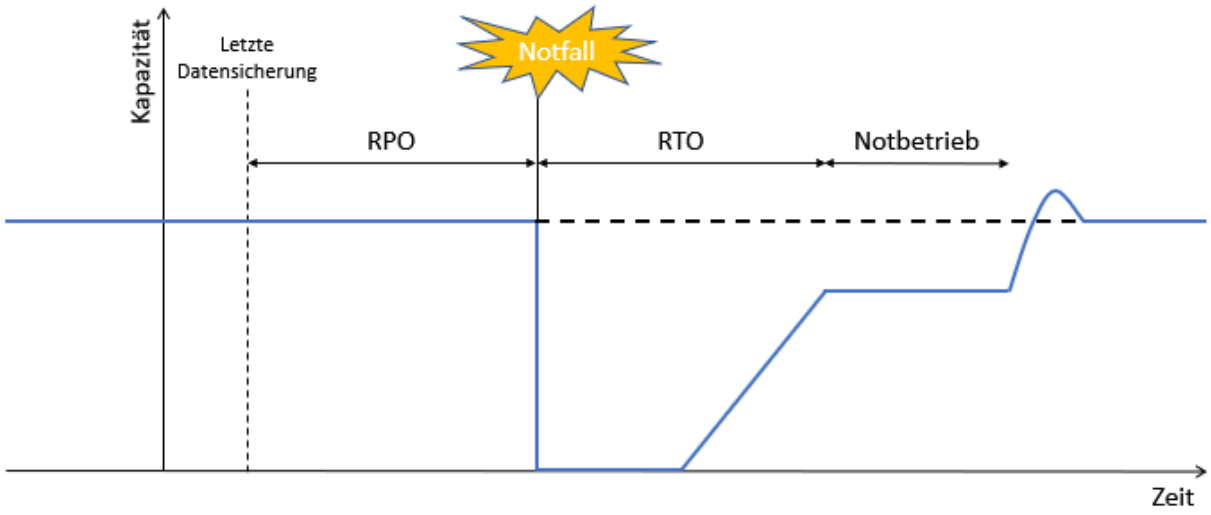


Abbildung 2: Disaster Recovery Ablauf[45]

2.3.2 IT-Notfallmanagement Standards

Für ein organisierte und funktionierende Notfallmanagementsysteme wurden weltweit mehrere Standards entwickelt. An dieser Stelle werden die beiden Standards BSI 100-4 und ISO 22301 vorgestellt, da sie jeweils national und international die größte Relevanz für Notfallmanagementsysteme haben.[46] Sie vermitteln beide wie ein Notfallmanagementsystem mitunter zu planen, betreiben oder auch kontinuierlich zu verbessern ist, um den Geschäftsbetrieb zu gewährleisten beziehungsweise wiederherzustellen.[47]

2.3.2.1. BSI-Standard 100-4

Das BSI hat 2008 den Standard 100-4 zum Notfallmanagement veröffentlicht. In diesem wird eine Methodik beschrieben wie ein Notfallmanagement etabliert und aufrechtgehalten werden kann. Der Standard baut auf den vorangegangenen BSI-Standards 100-1 (Managementsysteme für Informationssicherheit), 100-2 (IT-Grundschutz) sowie 100-3 (Risikoanalyse) auf und ergänzt diese. Zusätzlich zum Standard wurde vom BSI ein Umsetzungsrahmenwerk veröffentlicht, welches die Implementierung eines Notfallmanagementsystems nach BSI 100-4 konkretisiert.

Das BSI definiert den Notfallmanagementprozess mit den Schritten wie in Abbildung 3.

---

[45] Vgl. Bundesamt für Sicherheit in der Informationstechnik 2008.

[46] Vgl. Reuter 2018, S. 214.

[47] Vgl. Osterhage 2016, S. 2.

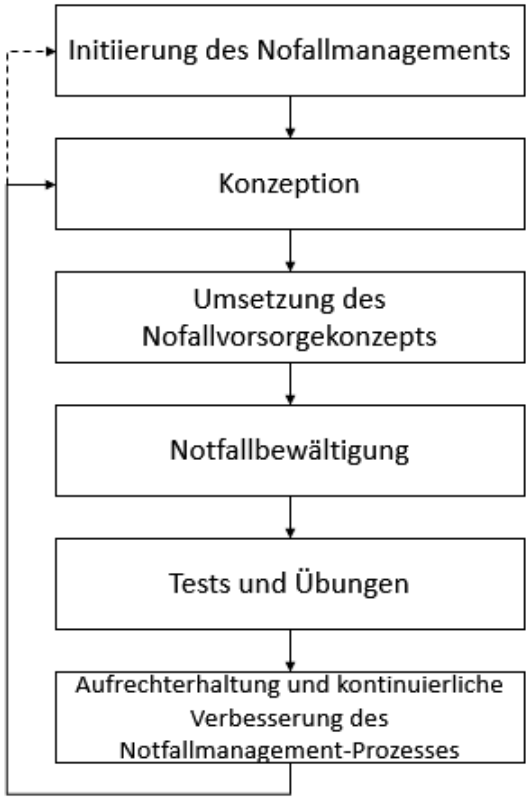


Abbildung 3: Notfallmanagementprozess nach BSI Standard 100-4[48]

Initiierung des Notfallmanagements: Am Anfang eines Notfallmanagementprozesses sollte die Verantwortung darüber an die Organisationsleitung übertragen werden. Diese ist verantwortlich für den ordentlichen Betrieb aller Geschäftsbereiche und ist befähigt die benötigten Ressourcen bereitzustellten. Sie muss sich deshalb der Bedeutung eines Notfallmanagementsystems bewusst sein.

Die Organisationsleitung legt den Geltungsbereich sowie die Zielsetzung des Notfallmanagementprozesses fest. Sie bestimmt zudem die verschiedenen Rollen und Personen in der Notfallvorsorgeorganisation.

Während der Initiierung ist die Organisationsleitung auch für die Erstellung einer Notfallleitlinie verantwortlich, in denen alle zuvor festgelegten Punkte zum Notfallmanagement festgehalten und für alle Mitarbeiter veröffentlicht werden.

Konzeption: Anschließend an die Initiierung wird eine BIA durchgeführt um über die Kritikalität, RPOs und RTOs aller Geschäftsprozesse Kenntnis zu haben. Zusammen mit einer

[48] Bundesamt für Sicherheit in der Informationstechnik 2008.

Risikoanalyse, bei der die Gefährdungen für die Geschäftsprozesse mit resultierenden Risiken identifiziert werden, können anschließend Kontinuitätsstrategien entwickelt werden. Mit diesen Kontinuitätsstrategien wird entschieden in welchem Umfang die einzelnen Prozesse beziehungsweise Systeme abgesichert werden.

Endprodukt der Konzeption ist ein Notfallvorsorgekonzept, das die einzelnen Ergebnisse dieses Prozessschrittes zusammenfasst und als Grundlage für die Umsetzung der Kontinuitätsstrategien dient.

Umsetzung des Notfallvorsorgekonzepts: Bevor die Umsetzung des Notfallvorsorgekonzepts beginnt, sind vorher die Kosten der einzelnen Maßnahmen zu schätzen. Sollten die prognostizierten Kosten das von der Organisationsleitung freigegebene Budget übersteigen, muss die Leitungsebene entscheiden ob zusätzliche Ressourcen zur Verfügung gestellt wird oder die Maßnahmen angepasst werden. Wenn die Kosten- und Aufwandsschätzung abgeschlossen ist, können die Verantwortlichen der einzelnen Maßnahmen und die Reihenfolge für die Umsetzung entschieden werden. Die Verantwortlichen haben dann die Vorsorgemaßnahmen umzusetzen.

Notfallbewältigung: Die Ablauforganisation wird festgelegt, damit nach einem Schadensereignis klar ist ob ein Notfall oder eine Krise ausgerufen wird und wer dafür verantwortlich ist. Dies, die Kommunikation während des Notfalls und sonstige Pläne für den Wiederanlauf der Prozesse werden in einem Notfallhandbuch niedergeschrieben.

Test und Übungen: Um sicherzustellen, dass die Pläne, welche während des Notfallmanagementprozesses ordentlich und schnell genug funktionieren, sollten regelmäßige Tests durchgeführt werden. Zudem sind, mithilfe von Übungen, die Mitarbeiter für den Notfall zu sensibilisieren und trainieren.

Aufrechterhaltung und kontinuierliche Verbesserung des Notfallmanagementprozesses: Der Notfallmanagementprozess muss von der Organisationsleitung in regelmäßigen Abständen evaluiert werden, um die Effektivität dessen stets gewährleisten zu können. Unter Hinzunahme der Ergebnisse aus den Tests und Übungen, sollte überprüft werden inwiefern der Prozess verbessert werden könnte.

2.3.2.2. ISO 22301

Die International Standard Organization (ISO) veröffentlichte 2012 den Standard 22301 für Anforderungen an *Business Continuity Managementsysteme* (BCM-System). Er stellt eine Weiterführung der ISO Standards 31000 (Risikomanagement) und 27001 (Informationssicherheitsmanagementsysteme) dar und löste den bisherigen *Business Continuity Management* Standard BS 25999 ab.[49] [50] Der Standard hat nicht das Ziel den Organisationen ein einheitliches BCM-System vorzugeben, da die ISO der Ansicht ist, dass BCM-Systeme nach den individuellen Bedürfnissen und Anforderungen gestaltet werden sollten.[51] Zu diesem Zweck beschreibt ISO 22301 wie ein BCM-System aufgebaut sein sollte ohne ins Detail der Umsetzung von Notfallprozessen einzugehen.

Wie auch andere Managementsystemstandards der ISO folgt die ISO 22301 einem *Plan-Do-Check-Act (PDCA) Modell*. Dadurch soll Konsistenz bei der Integration mit den teilweise zusammenhängenden anderen ISO-Standards gewährleistet werden. Das PDCA-Modell für BCM-Systeme, wie in Abbildung 4 zu sehen, funktioniert folgendermaßen. Interessengruppen definieren ihre Anforderungen an die Geschäftskontinuität und geben diese an das BCM-System. Anforderungen können beispielsweise Vorgaben zur RPO und RTO sein. Mithilfe dieser Anforderungen kann die Plan-Phase gestartet werden. Bei dieser Phase werden die Anforderungen in konkrete Richtlinien, Ziele und Prozesse zur Verbesserung der Geschäftskontinuität gewandelt. In der Do-Phase werden diese Vorgaben dann umgesetzt. Damit die Ergebnisse der BCM-Aktivitäten gemessen werden können, erfolgt eine Überwachung und Überprüfung dieser in der Check-Phase. Die Ergebnisse sind dem Management mitzuteilen, woraufhin dieses gegebenenfalls Veränderungen zur Verbesserung anordnet. Angeordnete Änderungen werden zuletzt dann in der Act-Phase umgesetzt. Diese vier Phasen wiederholen sich zyklisch und sorgen somit für eine kontinuierliche Verbesserung des Systems.

[49] Vgl. Osterhage 2016, S. 5.

[50] Vgl. Reuter 2018, S. 214.

[51] Vgl. International Organization for Standardization 2012.

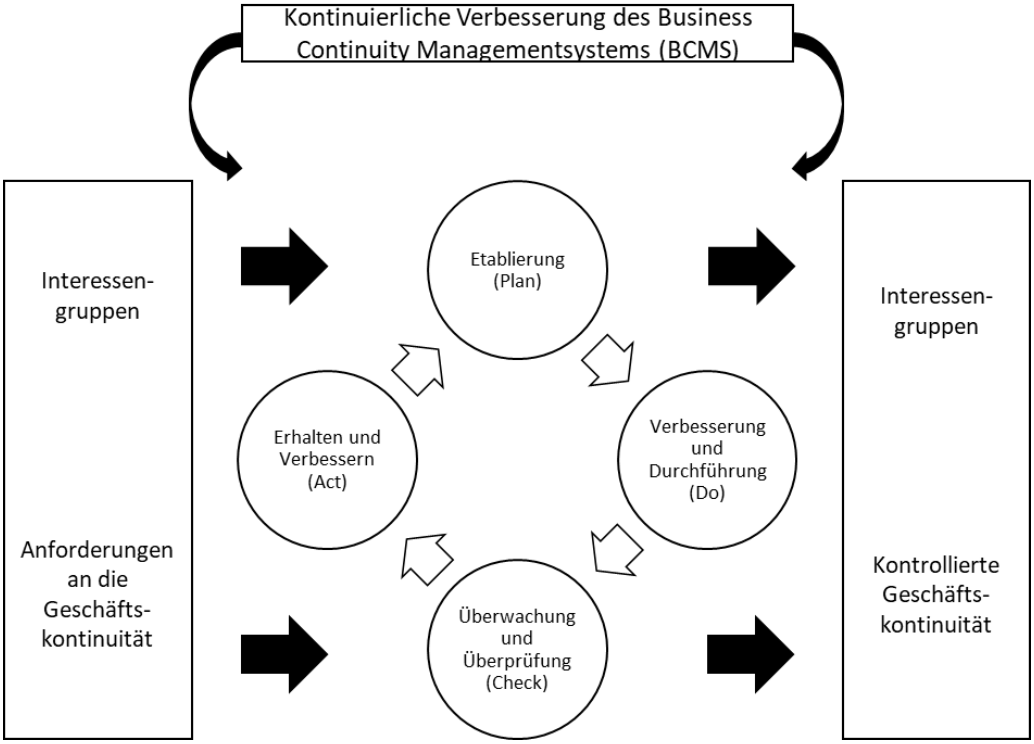


Abbildung 4: PDCA Modell für ein BCM-System[52]

2.3.3 Traditionelles Notfallmanagement

In diesem Kapitel wird die traditionelle Implementierung eines Notfallmanagements vorgestellt.

2.3.3.1. Definition

Mit *traditionellem Notfallmanagement* wird in dieser Arbeit ein Notfallmanagement bezeichnet, welches ohne den Einsatz von Cloud-Technologien auskommt. Daten als auch Systeme bleiben On-Premise in der nutzenden Organisation. Sollten die primären Systeme ausfallen bzw. drohen auszufallen, kann auf die Notfall-IT-Infrastruktur in einem Notfallrechenzentrum geschwenkt werden. Um geografisch zentriert wirkenden Notfallursachen entgegenzuwirken werden diese Notfallrechenzentren zudem oft georedundant aufgebaut. Das heißt die Notfallsysteme werden geographisch entfernt zum Hauptrechenzentrum bereitgestellt, um einen gleichzeitigen Ausfall von Primär- und Notfallrechenzentrum zu verhindern.[53]

[52] Vgl. International Organization for Standardization 2012.

[53] Vgl. Brotherton und Dietz 2014, S. 2.

2.3.3.2. Historie

Der Ansatz des traditionellen Notfallmanagements entwickelte sich aus dem Disaster Recovery, also der Wiederherstellung von Informationssystemen nach notfallbedingten Ausfällen. Während in der Vergangenheit nur die technische Seite betrachtet wurde, wird nun die Funktion dieser Systeme in den Vordergrund gestellt. Nach Supriadi und Sui Pheng entwickelte sich dies über die Zeit durch drei unterschiedliche Denkweisen.[54] In den 1970er Jahren bezog sich der Schutz von Informationssystemen fast ausschließlich auf die technische Hardware. Im darauffolgenden Jahrzehnt ging der Fokus auf die Benutzer der Hardware über. Es wurde angefangen Compliance-Regeln für die Nutzung einzuführen, welche durch regelmäßige Audits überprüft werden sollten. Ab den 1990er Jahren kam die wertorientierte Denkweise auf, welche sich nun auf die Geschäftsanforderungen fokussierte. Allmählich wurde erkannt, dass Notfallmanagement, oder auch BCM, nicht nur die Systeme absichert, sondern auch einen Wert für die Organisationen schaffen kann. Die Systeme wurden effizienter und Kunden konnten von höherer Zuverlässigkeit und Ausfallsicherheit profitieren. Abseits der Sicherung der Systeme entwickelte sich auch die Ansicht, dass das Notfallmanagement die ganze Organisation betreffen sollte. Insbesondere die Mitarbeiter sollten mehr eingebunden werden.

2.3.3.3. Standby-Lösungen

Für die Vorsorge eines Notbetriebs gibt es im traditionellen Notfallmanagement verschiedene Ansätze die benötigte Hardware bereitzustellen. Die folgenden vorgestellten Standby-Lösungen, fordern stets einen Kompromiss zwischen Kosten und Performanz.

Cold Standby

Die günstigste Strategie für einen Notfallstandort heißt *Cold Standby*. Notfallräumlichkeiten verfügen über eine Basisinfrastruktur, um einen längeren Ausfall des primären RZs zu kompensieren.[55] Mitunter müssen die Hardware bzw. Software jedoch erst beschaffen, installiert und konfiguriert werden, um die ausgefallenen Prozesse übernehmen zu können. Aus diesem Grund wird ein *kalter* Notfallstandort nicht parallel zum primären Standort

[54] Vgl. Supriadi und Sui Pheng 2018, S. 4–5.

[55] Vgl. Xiong et al. 2015.

betrieben. In der Zeit bis zur Funktionstüchtigkeit kann dabei ein erheblicher Schaden für die Organisation entstehen.[56] [57]

Warm Standby

Die Hardware ist bereits vorhanden, das heißt es muss im Notfall nichts Weiteres beschaffen werden. Eventuell muss die Hardware noch konfiguriert, sowie die Datensicherungen eingespielt werden.[58] Diese Lösung stellt die mittlere Alternative dar und bietet eine meist ausreichende Wiederherstellungsgeschwindigkeit zu gemäßigten Kosten.[59]

Hot Standby

Bei *Hot Standby* wird ein Notfallstandort mitsamt laufender Hard- und Software parallel zum primären Standort betrieben. Der sekundäre Standort verarbeitet, im Normalbetrieb, zwar keine Daten, jedoch werden diese mit dem primären Standort kontinuierlich synchronisiert. Sollte das primäre RZ ausfallen können die Prozesse mit sehr geringem Zeitverlust auf die Ersatzhardware schwenken.[60] Nachteil dieser Alternative sind die sehr hohen Kosten. Um RPO und RTO minimal zu halten müssen zusätzlich zum redundanten Nachbau des primären Rechenzentrums, die Daten zwischen beiden Standorten stets synchron gespiegelt werden.[61]

2.3.4 Notfallmanagement in der Cloud

In Kapitel 2.2.2 wurde erklärt wie IT-Infrastrukturen herkömmlich gegenüber Ausfällen abgesichert worden. Durch den Aufzug des Cloud Computing, ist heutzutage die Möglichkeit gegeben, IT-Infrastrukturen zu nutzen die durch andere Organisation betrieben und verwaltet werden. Inwiefern die Cloud genutzt werden kann, um Ausfälle der IT zu verhindern bzw. Schäden zu minimieren soll in diesem Kapitel behandelt werden.

Da eine Private Cloud On-Premise Ressourcen nutzt und der Notfallmanagement-Prozess sich nicht wesentlich vom traditionellen Notfallmanagement unterscheidet, sind in diesem Kapitel bei Verwendung des Begriffs *Cloud* hauptsächlich Public Clouds gemeint.

[56] Vgl. Kersten und Klett 2017, S. 119.

[57] Vgl. Bundesamt für Sicherheit in der Informationstechnik 2008.

[58] Vgl. Bundesamt für Sicherheit in der Informationstechnik 2008.

[59] Vgl. Kersten und Klett 2017, S. 119.

[60] Vgl. Kersten und Klett 2017, S. 119.

[61] Vgl. Wood et al. 2010.

2.3.4.1. Disaster Recovery as a Service (DRaaS)

Der gleichen Nomenklatur wie *Software as a Service*, *Platform as a Service* und *Infrastructure as a Service* folgend, ist *Disaster Recovery as a Service* (DRaaS) ebenfalls ein Cloud Servicemodell. Auch wenn DRaaS, anders als die in Kapitel 2.2.1 vorgestellten Servicemodelle, nicht vom NIST definiert wurde, hat sich der Begriff in der Literatur bereits gefestigt.[62] [63] Grundidee dieses Modells ist die Einbeziehung von Cloud-Systemen bei der Umsetzung eines Notfallplans. Das heißt im Notfall wird nicht auf redundante On-Premise IT-Infrastrukturen, sondern auf IT-Infrastrukturen in der Cloud geschwenkt. DRaaS erfreut sich zunehmender Beliebtheit, da es meist kostengünstiger gegenüber der Alternative, der Beschaffung und dem Betrieb eines redundanten Notfallrechenrechenzentrums, ist.[64] [65] Besonders vielen kleineren Organisationen und Unternehmen sind die Kosten eigener Notfallsysteme in der Vergangenheit zu hoch gewesen, sodass auf BCM und DR Pläne oft verzichtet wurde.[66] Mit DRaaS bietet sich ihnen nun eine günstige Möglichkeit ihre Geschäftskontinuität abzusichern.

Für die Wiederherstellung bei Nutzung von DRaaS gibt es verschiedene Strategien die nachfolgend vorgestellt werden. Für den Vergleich zwischen traditionellem und cloudbasiertem Notfallmanagementansatz wird in dieser Arbeit jedoch nur die Strategie *Replikation von VMs in die Cloud* herangezogen.

Backup in die Cloud und Restore aus der Cloud

Bei der technisch einfachsten Variante DR in die Cloud auszulagern, verbleiben Systeme als auch primäre Datenbestände On-Premise. Daten werden zusätzlich in der Cloud gespeichert um im Notfall, bei Nichtverfügbarkeit der primären Daten, aus der Cloud die Backup-Daten wieder einzuspielen. Die Cloud ersetzt damit das bisherige Speichern auf lokalen Speichern. Die Wiederherstellung aus der Cloud kann bei sehr großen Datenmengen problematisch werden, wenn das Herunterladen eine längere Zeit in Anspruch nimmt. Es muss deshalb darauf geachtet werden, dass eine Wiederherstellung innerhalb der geforderten RTOs der verschiedenen Systeme erfolgen kann.[67]

---

[62] Vgl. Andrade et al. 2017, S. 929.

[63] Vgl. Alhazmi 2016, S. 3.

[64] Vgl. Natarajan 2015, S. 193.

[65] Vgl. Gharat und Mhamunkar 2015.

[66] Vgl. Lenk 2014, S. 13.

[67] Vgl. Gsoedl 2011.

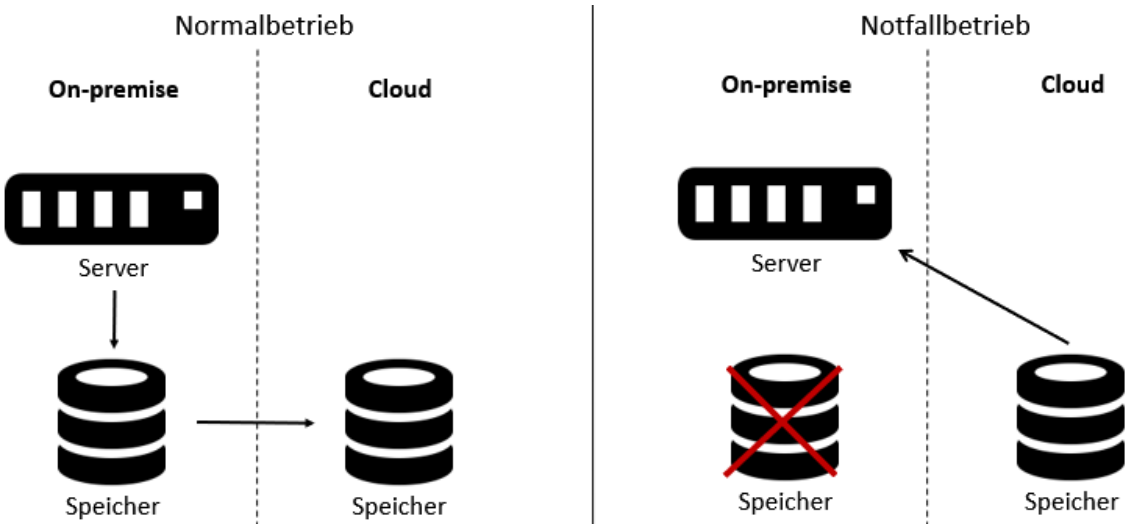


Abbildung 5: Backup in die Cloud und Restore aus der Cloud

Backup in die Cloud und Restore in die Cloud

Ähnlich wie bei *Backup in die Cloud und Restore aus der Cloud* bleiben die primären Systeme und Daten On-Premise. Die Daten werden zusätzlich zu den primären Beständen in der Cloud gesichert. Im Notfall werden die Daten aus der Cloud nicht auf die Systeme im Haus, sondern auf virtuelle Maschinen (VM) in der Cloud eingespielt. Dies hat einerseits zur Folge, dass die RTOs leichter einzuhalten sind und andererseits entfällt damit Notwendigkeit eines Notfallrechenzentrums.[68]

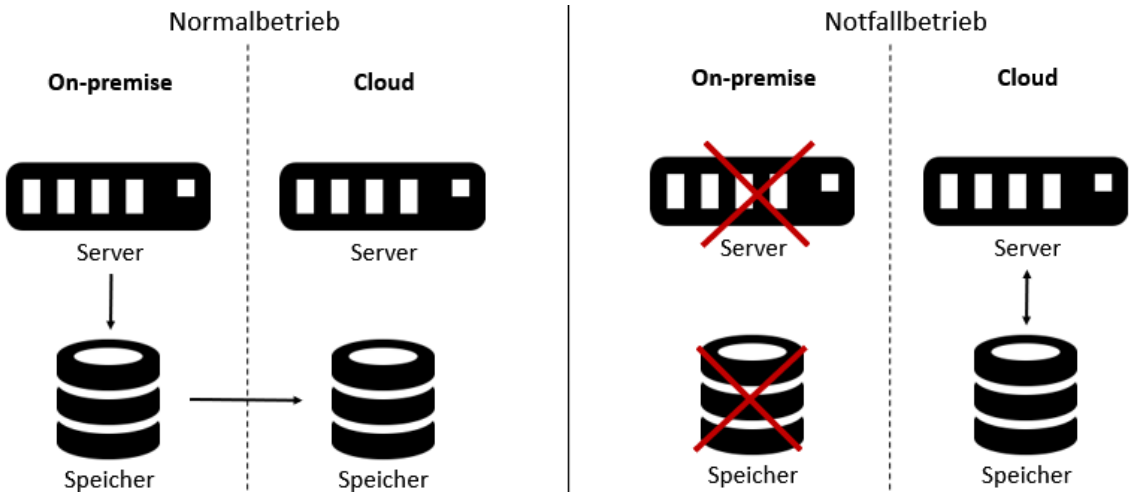


Abbildung 6: Backup in die Cloud und Restore in die Cloud

[68] Vgl. Gsoedl 2011.

Replikation von VMs in die Cloud

Virtuelle Maschinen mit den Anwendungen und Daten werden mit geringem Zeitabstand zu Servern des Cloudanbieters repliziert. Je nach Angebot kann die Replikation kontinuierlich oder mit Snapshots der VMs alle paar Minuten erfolgen. Die Anwendungen stehen im Notfall sofort auf den Cloudservern bereit und müssen nicht erst eingespielt werden. Diese Variante von DRaaS ist für besonders zeitkritische Anwendungen geeignet bei denen RTO und RPO sonst schwierig einzuhalten wären. Da auch hier der Notbetrieb in der Cloud abläuft, werden keine weiteren On-Premise Notfallkapazitäten benötigt.[69]

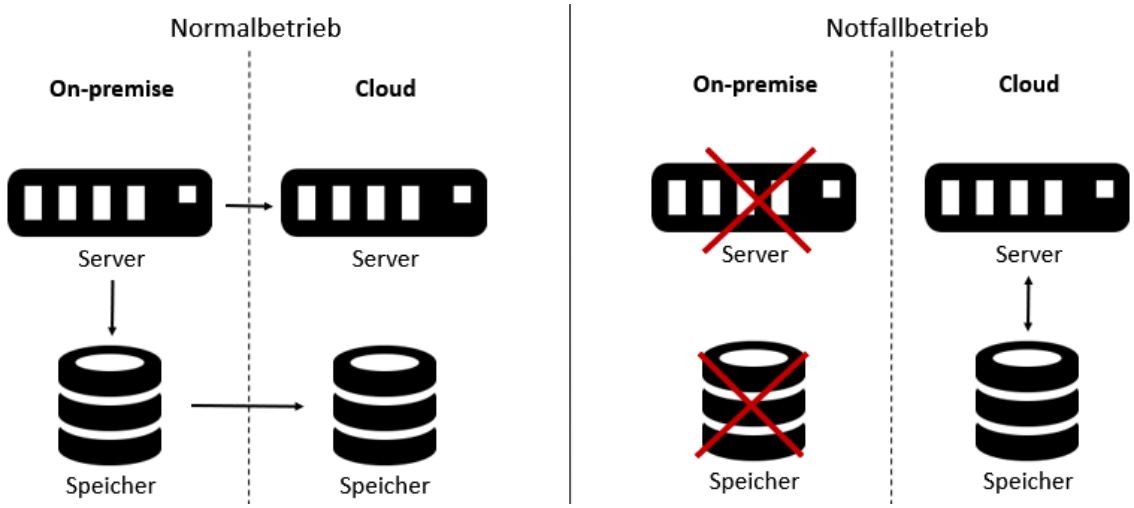


Abbildung 7: Replikation von VMs in die Cloud

2.3.4.2. Infrastructure as a Service (IaaS)

IaaS wurde bereits in Kapitel 2.2.1 vorgestellt und erläutert. Hier wird mehr auf die Bedeutung von IaaS für ein cloudbasiertes Notfallmanagement eingegangen.

Anders als bei allen Varianten von DRaaS, befindet sich fast die gesamte Hardware samt Infrastruktur, abgesehen von den Endgeräten, bei der dienstleistenden Organisation. Da die Nutzerorganisation nur die virtualisiert bereitgestellte IT-Infrastruktur verwaltet, nicht aber die darunterliegende physische IT-Infrastruktur, ist sie auch nicht für den Notfallmanagementprozess verantwortlich. Sollte der Notfall eintreten ist die Nutzerorganisation somit vollkommen abhängig von ihrem Dienstleister. Um sich trotz dessen

[69] Vgl. Gsoedl 2011.

gegenüber Notfällen abzusichern oder deren Auswirkungen zu minimieren, bleibt nur die Möglichkeit vertragliche Vereinbarungen mit dem Dienstleister zu treffen.

2.3.4.3. Aktuelle Marktsituation

Ähnlich wie der Markt für Cloudtechnologien im Allgemeinen stark wächst, vergrößert sich auch die Nachfrage nach einem ausgelagerten Notfallmanagement-Dienst. Laut einer Studie von *Markets and Markets* hatte der weltweite Markt für DRaaS im Jahr 2016 einen Umsatz von 1,72 Mrd. USD. Es wird erwartet, dass dieser Wert bis 2022 exponentiell auf 12,5 Mrd. USD steigen wird.[70] Zudem hat eine Befragung von 400 Unternehmen weltweit zu dem Thema ergeben, dass 80% aller Unternehmen bereits eine Form von DRaaS nutzen oder eine Einführung dessen planen. (s.Abb.8)

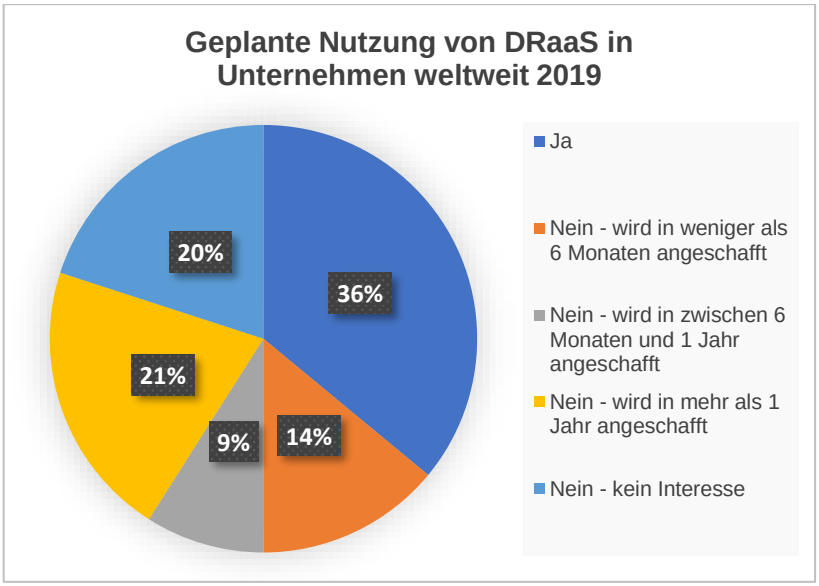


Abbildung 8: Nutzung von DRaaS weltweit 2019[71]

[70] Vgl. MarketsandMarkets 2017.

[71] Unitrends 2019.

3. Untersuchungsgegenstände

Die ausgewählten Untersuchungsgegenstände sollen Aufschluss darüber geben ob ein cloudbasiertes Notfallmanagement redundante Notfallrechenzentren des traditionellen Notfallmanagements ablösen können. Zusätzlich zu den zwei wichtigsten Messgrößen für ein gut funktionierendes Notfallmanagement, RPO und RTO, werden weitere Aspekte untersucht, die helfen das traditionelle und cloudbasierte Notfallmanagement miteinander zu vergleichen.

3.1 Kosten

Einer der wichtigsten Aspekte bei der Betrachtung von traditionellem und cloudbasiertem Notfallmanagement sind die Kosten, die für die Lösungen aufzuwenden sind. Für Entscheidungsträger einer Organisation ist es stets wichtig Kosten und Nutzen von Investitionen abzuwägen. Ein nur geringer Nutzengewinn einer der beiden Lösungen zu signifikant höheren Kosten gegenüber der Alternative kann deswegen zur Ablehnung der Lösung führen. Kosten lassen sich in Bereitstellungskosten und Kosten für den operativen Betrieb unterteilen. Bereitstellungskosten sind weiter zu unterteilen in Anschaffungskosten für die Hardware bzw. einmalige Kosten für Cloudressourcen und Implementierungskosten für die Inbetriebnahme. Der operative Betrieb setzt sich aus den laufenden Kosten für Ressourcen und Betriebspersonal zusammen. In der Literatur mangelt es noch an Untersuchungen, welche die Kosten von On-Premise und Cloud Notfall-IT-Infrastrukturen vergleichen. (Stand 2020) Es wurden jedoch Vergleiche zwischen allgemeinen On-Premise und Cloud IT-Infrastrukturen durchgeführt.

In einer Fallstudie von Nayar und Kumar konnten zwischen On-Premise und Cloudbetrieb durchaus signifikante Kostenunterschiede aufgezeigt werden.[72] Während die jährlichen Betriebskosten einer IT-Infrastruktur bei der On-Premise Implementierung 1.492.000INR (Indische Rupien) betrugen, kamen die Autoren bei der Cloudimplementierung auf 905,916INR. Unter der Annahme, dass die Betriebskosten zwischen On-Premise und Cloud Betrieb einer gesamten IT-Infrastruktur prozentual vergleichbar sind mit den Betriebskosten derer für eine reine Notfall-Infrastruktur, bedeutet dies einen Kostenaufschlag von ca. 65%. Für die Bereitstellungskosten wurden Werte von 742.900INR für On-Premise und 124.467INR für die Cloudimplementierung ermittelt was einen Kostenaufschlag von fast 500% gegenüber der Lösung in der Cloud bedeutet.[73]

[72] Vgl. Nayar und Kumar 2018, S. 14.

[73] Vgl. Nayar und Kumar 2018, S. 14.

Wood et al. haben in einer Fallstudie berechnet, dass ein redundantes Notfall-RZ laufende Mehrkosten von 42% zum primären RZ verursacht während ein DRaaS nur 6,5% an laufenden Mehrkosten bedeutet.[74] Aus den Ergebnissen der Fallstudien lässt sich ableiten, dass eine On-Premise IT-Infrastruktur gegenüber einer Cloud-IT-Infrastruktur höhere einmalige als auch höhere laufende Kosten verursacht.

3.2 Wiederherstellungspunkt (RPO)

Wie in Kapitel 2.3.1 beschrieben, ist die RPO eine der zwei zentralen Messgrößen für ein gut funktionierendes Notfallmanagement.[75] Sie wird von der Organisation vorgegeben und bedeutet die Zeitspanne, die seit der letzten Datensicherung maximal vergehen darf, wenn der Notfall eintritt. Das heißt die RPO bestimmt das Intervall in dem Datensicherungen durchzuführen sind.[76] Wood et al. schreiben, dass eine kurze RPO für datenintensive Anwendungsfällen zu höheren Kosten bei der Nutzung von Cloud-Diensten führt, da die Cloud-Ressourcen dadurch fast kontinuierlich gemietet werden müssen. Trotz dessen ist es nach seiner Fallstudie möglich eine kontinuierliche Replikation in die Cloud zu geringeren Kosten gegenüber der On-Premise Lösung zu realisieren.[77]

Ein weiterer Aspekt, der die RPO beeinflussen könnte, ist die Geschwindigkeit der Verbindung zwischen primären und Notfallsystemen. Da die Geschwindigkeit mitunter von der Distanz zwischen den Systemen abhängt, kann eine große Entfernung, wie sie zwischen Cloudnutzer und Cloudanbieter auftreten könnte, zu einer langsameren Synchronisationsrate führen. Andererseits bedeutet eine Entfernung zwischen primären und Notfallsystemen auch, dass die Systeme georedundant aufgebaut sind, was wiederum einen Sicherheitsgewinn bedeutet, da lokale notfallbewirkende Ereignisse nicht beide Standorte betreffen werden.[78] Auch redundante On-Premise Notfallrechenzentren sollten also gewissermaßen entfernt betrieben werden. Eine geringere Synchronisationsrate aufgrund großer Distanz ist demnach nicht unbedingt ein Nachteil von DRaaS. Zusammenfassend unterscheidet sich die mögliche RPO bei DRaaS nicht sonderlich von der beim traditionellen Notfallmanagement und kann durch erhöhten Kapitaleinsatz ein ähnliches Niveau erreichen.

[74] Vgl. Wood et al. 2010.

[75] Vgl. Andrade et al. 2017, S. 938.

[76] Vgl. Lenk 2014, S. 51.

[77] Vgl. Wood et al. 2010.

[78] Vgl. Alhazmi und Malaiya 2013, S. 4.

3.3 Wiederherstellungszeit (RTO)

Die zweite zentrale Messgröße im Notfallmanagement, RTO, bezeichnet die Zeit, die nach einem Notfall maximal bis zu einer Wiederherstellung der Systeme vergehen darf. Sie wird ebenso wie die RPO von der Organisation vorgegeben und richtet nach Kritikalität des IT-Betriebs. Beim Vergleich der RTO bei traditionellem Notfallmanagement und DRaaS ist anzumerken, dass die RTO des traditionellen Notfallmanagements stark von der implementierten Standby-Lösung (siehe Kapitel 2.3.3.3) abhängt. Eine Hot Standby Lösung ermöglicht zum Beispiel eine kürzere RTO als eine Cold Standby Lösung, ist dafür mit höheren Kosten verbunden. Wie auch bei der RPO ist es hierbei wichtig zu wissen was die Geschäftsanforderungen sind, um eine adäquate Notfallstrategie zu planen.[79] Sind die Anforderungen an die RTO niedrig sollte man aus Kostengründen auch beim traditionellen Notfallmanagement keine Hot Standby Lösung implementieren. In ihrem Paper schreiben Wood et al., dass DRaaS bei Anwendungsfällen mit sehr geringer RTO dahingehend keinen Vorteil gegenüber einer Hot Standby Lösung bietet. Sie beziehen sich hierbei auf die durchschnittliche Startdauer von 200s einer virtuellen Maschine in einer Amazon EC2 Cloud.[80] Auch Lenk merkt an, dass bei einer sehr kritischen RTO eine Hot Standby Lösung aufgrund des schnelleren Wiederanlaufs der Systeme gegenüber DRaaS präferiert werden sollte.[81] Abschließend lässt sich sagen, dass sich mit DRaaS eine RTO erreichen lässt die zwischen der von Hot und Warm Standby liegt. Da die Bereitstellungs- als auch laufenden Kosten von DRaaS vermutlich geringer sind als die eines Warm Standby Notfallrechenzentrums, ist ein traditionelles Notfallmanagement hinsichtlich RTO nur bei sehr kritischen Anwendungsfällen vorteilhafter.

3.4 Datensicherheit

Die Datensicherheit ist ein Thema welches nicht nur für die Nutzung von DRaaS, sondern auch für die allgemeine Nutzung von Cloud Computing wichtig ist. Während bei einer On-Premise IT-Infrastruktur und beim traditionellem Notfallmanagement alle Daten und Systeme in der eigenen Organisation verwaltet werden, muss sich die nutzende Organisation bei Cloud und DRaaS teilweise auf die Sicherheit der Dienstleister verlassen und diesen vertrauen.[82] [83] Für

[79] Vgl. Andrade et al. 2017, S. 948.

[80] Vgl. Wood et al. 2010.

[81] Vgl. Lenk 2014, S. 214.

[82] Vgl. Lenk 2014, S. 237.

[83] Vgl. Gharat und Mhamunkar 2015.

Organisationen die kritische bzw. hochkritische Daten verwalten, kann dies ein Problem darstellen da die Gefahr besteht, dass beauftragte Cloud-Dienstleister auf die Daten zugreifen. Durch Gesetze, die es Staaten erlauben auf Daten von diesen Dienstleistern wird dieses Sicherheitsrisiko zudem gestärkt.[84] [85] Ein weiteres Risiko besteht darin, dass die IT nicht mehr durch die organisationsinterne Netzwerksicherung gegen externe Angreifer geschützt wird. Traditionell werden Unternehmensnetzwerke durch interne Firewall, DMZ und externe Firewall von nicht autorisierten Zugriffen aus dem Internet abgesichert.[86] Bei DRaaS ist der Cloud-Dienstleister verantwortlich für diese Absicherung. Andererseits schreibt Bedner, die IT und Daten können durch Cloud Computing sicherer gegen externe Angreifer geschützt werden, da Cloud-Dienstleister in bestimmten Fällen ihre Systeme besser absichern.[87] Er argumentiert damit, dass Cloudanbieter und ihre Mitarbeiter spezialisierter im Schutz von IT-Systemen sind als beispielsweise kleine Unternehmen. Es lässt sich abschließend sagen, dass das traditionelle Notfallmanagement eine größere Kontrolle über Daten erlaubt als DRaaS.

3.5 Datenschutz

Unternehmen und andere Organisationen sind in Deutschland schon länger verpflichtet Personendaten nicht für anderweitige Zwecke, als den von Kunden beauftragten, zu missbrauchen. Durch das Inkrafttreten der EU-weit geltenden Datenschutz-Grundverordnung (DSGVO) haben sich die Anforderungen an die Personendaten-verarbeitenden Organisationen nur erhöht.

In Bezug auf die Nutzung von Cloud-Services, wird nach DSGVO zwischen Verantwortlichem und Auftragsverarbeitendem unterschieden. Verantwortlicher ist wer "über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“[88]. Auftragsverarbeitender ist wer "personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet" [89]. Beim Einsatz von Cloudspeichern, wäre die nutzende Organisation der Verantwortliche und die ressourcenbereitstellende Organisation Auftragsverarbeitender.[90] Laut Verordnung ist der Verantwortliche in der Pflicht nur mit Auftragsverarbeitenden zu arbeiten die den Schutz

[84] Vgl. Avram 2014, S. 533.

[85] Vgl. Wood et al. 2010.

[86] Vgl. Surianarayanan und Chelliah 2019, S. 190.

[87] Vgl. Bedner 2013, S. 95.

[88] Europäische Union 2016.

[89] Europäische Union 2016.

[90] Vgl. Voigt und dem Bussche 2018, S. 315.

personenbezogener Daten durch technische und organisatorische Maßnahmen gewährleisten können. Cloudnutzer, im Falle vom cloudbasierten Notfallmanagement die nutzende Organisation, müssen also ihre Dienstleister auf Erfüllung dieser Maßnahmen überprüfen und sie zur Einhaltung der Datenschutzbestimmungen vertraglich verpflichten.[91] Für DRaaS bedeutet dies, dass die nutzende Organisation zusätzlich zur Einhaltung der DSGVO bei ihren primären Systemen noch den Cloudanbieter auf Konformität prüfen muss.

[91] Vgl. Voigt und dem Bussche 2018, S. 316.

4. Resümee

Ein traditionelles Notfallmanagement mit seinen redundanten IT-Ressourcen ist für viele Organisationen ein recht kostspieliges, jedoch notwendiges Unterfangen, um Ausfälle der IT und damit einhergehende Störungen des Geschäftsbetriebs zu vermeiden. Diese Arbeit hatte das Ziel Aufschluss darüber zu geben ob eine Verlagerung des Disaster Recovery in die Cloud diesen Kostenfaktor minimieren kann und andererseits dieselben Effektivität erzielt. Dazu wurden die beiden Methoden anhand verschiedener Aspekte untersucht und miteinander verglichen.

Der Vergleich hat gezeigt, dass traditionelles und cloudbasiertes Notfallmanagement nur geringe Unterschiede in Bezug auf möglichen *Wiederherstellungspunkt* (RPO) und *Wiederherstellungszeit* (RTO) aufweisen. Hierbei ist jedoch anzumerken, dass beide Aspekte stark abhängig von den *Kosten* sind, die aufgewendet werden. Insgesamt lässt sich aber sagen, dass zu ähnlichen Werten geringere Kosten beim cloudbasierten Notfallmanagement anfallen. Nur sehr niedrige Wiederherstellungszeiten lassen sich durch ein traditionelles Notfallmanagement besser realisieren, da das cloudbasierte Notfallmanagement eher einem Warm Standby ähnelt, während bei der On-Premise Variante auch eine Hot Standby Lösung möglich ist bei der keine Systeme mehr hochgefahren werden müssen.

Zum Untersuchungsgegenstand *Kosten* lässt sich auch abgesehen von RTO und RPO sagen, dass ein cloudbasiertes Notfallmanagement in den meisten Fällen kostengünstiger als ein traditionelles Notfallmanagement ausfällt. Auch wenn sich die laufenden Kosten verhältnismäßig wenig unterscheiden, so hat der Vergleich gezeigt, dass die Bereitstellungskosten von redundanten IT-Ressourcen ein Vielfaches der einmaligen Kosten von DRaaS bedeuten.

Die letzten beiden Untersuchungsgegenstände *Datensicherheit* und *Datenschutz* zeigten das Risiko auf, das aus der Nutzung von organisationsfremden IT-Ressourcen hervorgehen kann. Organisationen, deren Daten und Systeme besonders kritisch sind, werden womöglich weiterhin eher auf ihre organisationsinterne IT-Sicherheit vertrauen als ihre Daten in der Cloud zu speichern.

Obwohl der Markt des cloudbasierten Notfallmanagement weiterhin stark wächst, konnte der Vergleich nicht zeigen, dass das traditionelle Notfallmanagement dadurch obsolet wird. Wie auch On-Premise IT-Infrastrukturen noch nicht für alle Anwendungsfälle ihre Daseinsberechtigung verloren haben, gibt es auch für das traditionelle Notfallmanagement mit redundanten Rechenzentren noch gute Gründe. Da RPO und RTO keine großen Unterschiede aufweisen, ist die Wahl zwischen beiden Varianten stets ein Kompromiss zwischen Kosten und Datensicherheit. Die DSGVO-Konformitätsprüfung des Clouddienstleisters bedeutet zwar

einen Mehraufwand bei DRaaS, dieser ist aber vermutlich vernachlässigbar da Zertifizierungen für die Dienstleister diesen Aufwand minimieren werden.

Es lässt sich abschließend sagen, dass ein cloudbasiertes Notfallmanagement aufgrund deutlich niedrigerer Kosten für jede Organisation zu empfehlen ist die eine Reduktion der Datensicherheit verkraften kann. Organisationen, wie beispielsweise Behörden deren Daten hochkritisch sind, werden nur schwierig bereit sein ihre Daten in eine Public Cloud zu migrieren. Inwiefern sich das Cloud Computing verändert und damit auch sicherheitsskeptischen Organisationen eine Möglichkeit bietet cloudbasiertes Notfallmanagement zu nutzen könnte in zukünftigen Forschungsarbeiten erforscht werden.

5. Literaturverzeichnis

Alhazmi, Omar H. (2016): A Cloud-Based Adaptive Disaster Recovery Optimization Model. In: *CIS* 9 (2), S. 58

Alhazmi, Omar H.; Malaiya, Yashwant K. (2013): Evaluating Disaster Recovery Plans Using the Cloud. Piscataway, NJ: IEEE

Andrade, Ermeson; Nogueira, Bruno; Matos, Rubens; Callou, Gustavo; Maciel, Paulo (2017): Availability modeling and analysis of a disaster-recovery-as-a-service solution, S. 929–954

Avram, M. G. (2014): Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective

Baun, Christian; Kunze, Marcel; Nimis, Jens; Tai, Stefan (2011): Cloud Computing. Berlin, Heidelberg: Springer Berlin Heidelberg

Bedner, Mark (2013): Cloud Computing. Technik, Sicherheit und rechtliche Gestaltung. Kassel: Kassel University Press (Forum Wirtschaftsrecht, Band 14)

Brotherton, H.; Dietz, J. (2014): Data Center Site Redundancy. In: *10th International Conference of the International Institute for Infrastructure Resilience and Reconstruction (I3R2)*, S. 2–6

Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4

Dillon, Tharam; Wu, Chen; Chang, Elizabeth (2010): Cloud Computing: Issues and Challenges. In: *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, S. 27–33

Erb, Simon (2015): Business Continuity Management in Outsourcing-Beziehungen. Dissertation

Europäische Union (2016): VERORDNUNG (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung). DSGVO

Gandhi, Vaibhav; Kumbharana, Chandresh (2018): Comparative study of Amazon EC2 and Microsoft Azure cloud architecture. In: *International Journal of Advanced Networking Applications (IJANA)*

Gharat, Akshay; Mhamunkar, Devendra (2015): Disaster Recovery in Cloud Computing

Gsoedl, Jacob (2011): Disaster recovery in the cloud explained. Online verfügbar unter https://searchdisasterrecovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained, zuletzt geprüft am 09.01.2020

Hintermann, Ralph; Clausen, Jens (2014): Rechenzentren in Deutschland: Eine Studie zur Darstellung der wirtschaftlichen Bedeutung und der Wettbewerbssituation

Hossny, Eman; Khattab, Sherif; Omara, Fatma; Hassan, Hesham (2013): A Case Study for Deploying Applications on Heterogeneous PaaS Platforms

International Organization for Standardization (2011): ISO/DIS 22313. Societal security — Business continuity management systems — Guidance

International Organization for Standardization (2012): ISO 22301

Kersten, Heinrich; Klett, Gerhard (2017): Business Continuity und IT-Notfallmanagement. Grundlagen, Methoden und Konzepte. Wiesbaden: Springer Fachmedien Wiesbaden

Kohne, Andreas (2018): Cloud-Föderationen. SLA-basierte VM-Scheduling-Verfahren. Wiesbaden: Springer Fachmedien Wiesbaden

Laudon, Kenneth C.; Laudon, Jane Price; Schoder, Detlef (2016): Wirtschaftsinformatik. Eine Einführung. 3., vollständig überarbeitete Auflage. Hallbergmoos: Pearson (Always learning)

Lenk, Alexander (2014): Cloud Standby. Eine Methode zur Vorhaltung eines Notfallsystems in der Cloud

MarketsandMarkets (Hg.) (2017): Global Disaster recovery as a service (DRaaS) Market. Size, Growth, Trends, Industry Analysis, Forecast 2022. Online verfügbar unter https://www.marketsandmarkets.com/Market-Reports/recovery-as-a-service-market-962.html, zuletzt geprüft am 09.01.2020

Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand (2011): Cloud computing — The business perspective. In: *Decision Support Systems* 51 (1), S. 176–189

Mell, P. M.; Grance, T. (2011): The NIST definition of cloud computing. Gaithersburg, MD: National Institute of Standards and Technology

Münzl, Gerald; Pauly, Michael; Reti, Martin (2015): Cloud Computing als neue Herausforderung für Management und IT. Berlin: Springer Vieweg (essentials)

Natarajan, R. (Hg.) (2015): Proceedings of the International Conference on Transformations in Engineering Education. ICTIEE 2014. New Delhi, s.l.: Springer India

Nayar, Kiran Bala; Kumar, Vikas (2018): Cost benefit analysis of cloud computing in education. In: *IJBIS* 27 (2), S. 205

Osterhage, Wolfgang W. (2016): Notfallmanagement in Kommunikationsnetzen. Berlin, Heidelberg: Springer Berlin Heidelberg (Xpert.press)

Reuter, Christian (Hg.) (2018): Sicherheitskritische Mensch-Computer-Interaktion. Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement. Wiesbaden: Springer Fachmedien Wiesbaden

Rudolph, Simone (2009): Servicebasierte Planung und Steuerung der IT-Infrastruktur im Mittelstand. Informationsmanagement und Computer Aided Team. Ein Modellansatz zur Struktur der IT-Leistungserbringung. 1. Aufl. s.l.: Gabler Verlag (Informationsmanagement und Computer Aided Team)

Stanoevska-Slabeva, Katarina (2010): Grid and cloud computing. A business perspective on technology and applications. Heidelberg: Springer

Subashini, S.; Kavitha, V. (2011): A survey on security issues in service delivery models of cloud computing. In: *Journal of Network and Computer Applications* 34 (1), S. 1–11

Supriadi, Leni Sagita Riantini; Sui Pheng, Low (2018): Business Continuity Management in Construction. Singapore: Springer Singapore (Management in the Built Environment)

Surianarayanan, Chellammal; Chelliah, Pethuru Raj (2019): Essentials of Cloud Computing. Cham: Springer International Publishing

Unitrends (2019): Planned usage of cloud-based DRaaS in companies worldwide 2019. Online verfügbar unter https://www.statista.com/statistics/1024437/worldwide-cloud-usage-disaster-recovery-as-a-service/, zuletzt geprüft am 09.01.2020

Voigt, Paul; dem Bussche, Axel von (2018): EU-Datenschutz-Grundverordnung (DSGVO). Berlin, Heidelberg: Springer Berlin Heidelberg

Watters, Jamie (2014): Disaster recovery, crisis response, and business continuity. A management desk reference. Berkeley, Calif.: Apress

Wood, Timothy; Shenoy, Prashant; Cecchet, Emmanuel (2010): Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges

Xiong, Huanhuan; Pahl, Claus; Fowley, Frank (2015): An Architecture Pattern for Multi Cloud High-Availability and Disaster Recovery