MASTERARBEIT

Kennzahlen im Kontext des Infrastruktur Monitorings

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Claudio Knapp

Personenkennzeichen: 2010320005

Graz, am 15. Dezember 2021 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Hiermit möchte ich mich in allererster Linie bei meiner Partnerin für die unglaublich tolle Unterstützung im Laufe des Studiums und Masterarbeit bedanken. Dies half mir ungemein, meinen Fokus auf die Fertigstellung der Mastarbeit zu lenken, auch wenn es nicht immer so leicht war.

Zudem gilt Herrn DI Dr. Softic, den Betreuer dieser Arbeit, ein großes Dankeschön für die investierte Zeit zur Beantwortung allermöglichen unklaren Sachverhalte und vielen hilfreichen Inputs im Rahmen der Abwicklung.

Weiters bedanke ich mich noch bei allen Experten, welche bei den durchgeführten Interviews zur Verfügung standen und mit all ihrem Wissen und Erfahrungen geholfen haben, einen wertvollen Beitrag für diese Arbeit zu leisten.

Abschließend gilt noch meinen Freunden und engen Begleitern im Studium ein Riesendank. Ihr habt mir geholfen unklare Sachverhalte zu lösen und immer schnell und zuverlässig auf Nachfragen reagiert. DANKE!

Claudio Knapp

KURZFASSUNG

Die Situation, welche COVID-19 hervorgerufen hat, drängte viele Organisationen dazu, ihre Arbeitsabläufe so weit als möglich vom ständigen Arbeitsort, auf das Homeoffice mittels Teleworking Arbeitsplätzen zu verlegen. Diese Maßnahme soll helfen, die Ausbreitung der Infektionskrankheit zu verlangsamen und einzudämmen.
Jedoch stellt dies den laufenden IT-Betrieb vor große Herausforderungen, wie die Erfüllung der im IT-Service Management definierten Ziele und Kennzahlen.
Die Einhaltung geforderter Grenzwerte ist essentiell um einen reibungslosen Ablauf der Geschäftsprozesse gewährleisten und somit die Organisation als Ganzes weiterführen zu können.
Auf Basis dieser Situation wird im Rahmen dieser Arbeit die Forschungsfrage „Wie haben sich mit vermehrtem Einsatz von Teleworking Arbeitsplätzen in der Pandemie von COVID-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert?“ behandelt.
Beginnend mit der Literaturrecherche werden Themenblöcke rund um IT-Service Management IT-Governance, IT-Performance-Management, IT-Ziele, Key-Performance-Indikatoren, Continual-Service-Improvement und den gängigen IT-Rahmenwerken beschrieben.
Darauffolgend werden die Themen Monitoring und den dazugehörigen Teilgebieten Infrastruktur, Cloud Service Modellen, Technologien und Tools sowie Knackpunkte des interdisziplinären Monitorings erörtert.
Abschließend für die Literaturrecherche wird eine Situationsanalyse der Pandemie von COVID-19 dargelegt und die daraus resultierenden Auswirkungen und korrigierenden Maßnahmen dargelegt.
Im fünften Teil der Arbeit werden die Hypothesen auf Basis der erarbeiteten Literatur erläutert.
Darauffolgend wird im sechsten Teil auf das Untersuchungsdesign erklärt. Hierzu gehören eine Beschreibung des Vorgehens selbst, die Befragte Untersuchungsgruppe, Kontaktaufnahme, Aufbau des Gesprächsleitfadens, Dokumentation der Durchführung und die Auswertung.
Zusammenfassend werden im siebten Kapitel die Ergebnisse erläutert.
Die durchgeführten Experteninterviews sind im Anhang enthalten und werden zusätzlich als Audioaufnahme der CD beigelegt.

ABSTRACT

COVID-19 has forced organisations to embrace online teleworking. This challenges ongoing IT operations regarding compliance with IT service management's defined goals and key performance indicators (KPIs). This research explores compliance with IT operations' KPIs to ensure business processes continue unimpeded. The research question addressed is "How have the requirements for monitoring metrics for IT operations changed with increased use of teleworking workplaces in the pandemic of COVID-19? ". Building on a literature review, this paper describes topics related to IT service management, such as IT governance, IT performance management, IT goals, KPIs, continuous service improvement, and two commonly used frameworks. Subsequently, monitoring and the associated sub-areas of infrastructure, cloud service models, technologies, and tools, as well as the key points of interdisciplinary monitoring are discussed. Finally, the COVID-19 pandemic is described for the literature review and the effects and countermeasures presented. The thesis continues by explaining the hypotheses using the literature review as context and explaining the interviews' research methodology, the interview guide, and the description of the four expert interview participants.

The final chapter summarises the findings. The integration of multiple mobile workplaces into the IT infrastructure and monitoring system triggered significant changes to the specified KPIs. The requirements in the context of security, integration of cloud services, network monitoring, client management, and performance management itself were affected.

INHALTSVERZEICHNIS

1 EINLEITUNG

Bedingt der vergangenen Auswirkungen von COVID-19 auf Arbeitsplätze und Kontaktbeschränkungen im Zuge der Pandemie, haben Organisationen mit der Verlagerung von konventionellen Arbeitsplätzen in Büros zu Teleworking Arbeitsplätzen begonnen. Diese, teils kurzfristige, Umstellung birgt neben Vorteilen auch enorme Risiken im Lichte der IT-Sicherheit. Hierbei haben gewartete und intensiv betreute Monitoringsysteme ihre Daseinsberechtigung, da sie helfen auf Gefahren in der Bereitstellung von IT-Infrastruktur und Services hinzuweisen, und optimalerweise proaktiv aufzuzeigen. Dieser Ansatz führt zur Untersuchung im Rahmen dieser Arbeit, und soll Organisationen helfen zu verstehen welche Auswirkungen die Pandemie auf die Kennzahlen von Monitoringsystemen hat.

1.1 Ausgangssituation

In Anbetracht der sich wandelnden Arbeitswelt und den Auswirkungen von Sicherheitsvorkehrungen bezüglich der Coronavirus Pandemie seit dem Jahr 2019, gewinnt Teleworking rasant an Bedeutung für unterschiedliche Branchen und Unternehmen. Aufgrund der Empfehlungen vom Bundesamt für Sicherheit in der Informationstechnik

Bei dem BSI (Bundesamt für Sicherheit in der Informationstechnik, 2008) sowie Rensmann & Gröpler (Rensmann & Gröpler, 1998) wird verstärkt Fokus auf die Bereitstellung von Infrastruktur für die Durchführung ortsunabhängiger Arbeit gesetzt. Diese Infrastruktur muss regelmäßig gewartet und im besten Fall mittels einer Monitoringlösung überprüft werden, ob sie die festgelegten Leistungsmerkmale (Olbrich, 2008) laut Spezifikationen noch zur Gänze erfüllt werden oder es zu Leistungsproblemen wie laut ITIL Richtlinien beschrieben wird kommt (Klosterboer, 2008).

Hierbei gilt es zu beachten, dass eine heterogene Arbeitsumgebung (in Bezug auf die verwendeten Werkzeuge zur Durchführung der Organisationsprozesse) auch unterschiedliche Anforderungen an Infrastruktur stellt (Addy, 2007). Weiterführend stellen auch sich veränderte Datenströme in und aus einer Organisation geänderte Erfordernisse an Infrastruktur und IT-Services selbst (International Labour Office, 2020).

Diese Herausforderungen führen zum Bedarf einer einheitlicher und zentralen Monitoringlösung, welche erforderliche Kennzahlen überwacht, sammelt und darstellt.

1.2 Forschungsziel

Im Rahmen dieser Masterarbeit wird, aufgrund der beschriebenen Veränderung der Anforderungen an Infrastruktur zur ortsunabhängigen Durchführung der Organisationsprozesse, ein, auf Bedürfnisse heterogener IT-Architekturen angepasster Kennzahlenkatalog für den Einsatz in einer Monitoringlösung erforscht. Auf Basis der Literaturrecherche und den daraus gewonnenen Erkenntnissen werden die Anforderungen einer heterogenen Serviceumgebung sowie Infrastruktur an eine Monitoringumgebung näher betrachtet.

Hierbei ist die Zielstellung der Masterarbeit, Organisationen mit Teleworking Arbeitsplätzen eine Empfehlung für eine Liste von Kennzahlen auszusprechen, welche für das IT-Servicemanagement eine Hilfestellung bieten soll, um eine potentielle Monitoringlösung dahingehend anzupassen und die festgelegte Leistungsfähigkeit gewährleisten zu können. Diese Zielsetzung wird mit folgender Forschungsfrage untersucht:

„Wie haben sich mit vermehrtem Einsatz von Teleworking Arbeitsplätzen in der Pandemie von COVID-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert?“

1.3 Aufbau der Arbeit

Die Arbeit gliedert sich neben dem Einleitungskapitel noch in drei Literaturkapitel sowie fünf Kapitel zum Untersuchungsvorgehen und der abschließenden Ergebnisse.

Beginnend mit dem zweiten Kapitel wird die Thematik rund um IT-Service-Management behandelt. Es werden die Begriffe definiert sowie IT-Governance, IT-Performance-Management, IT-Ziele und Key-Performance-Indikatoren behandelt. Weiters wird die Rolle des Continual-Service-Improvement im Kontext des IT-Service-Management beleuchtet. Abschließend wird auf zwei Rahmenwerke der IT, ITIL und COBIT, genauer eingegangen und ausschnittsweise Bausteine der Rahmenwerke mit Bezug zum Themenschwerpunkt dargelegt.

Im dritten Kapitel werden das Monitoring selbst, Monitoring im Kontext von Infrastruktur und Cloud Service Modelle definiert sowie Knackpunkte von interdisziplinärem Monitoring beleuchtet und die Lösung Microsoft System Center Operations Manager beschrieben.

Darauffolgend werden im vierten Kapitel eine Situationsanalyse der Pandemie mit Auswirkungen auf Organisationen und Maßnahmen zur Weiterführung des Betriebs ausgeführt.

Auf Basis dieser Informationen werden im fünften Kapitel die Hypothesen erstellt.

Im sechsten Kapitel wird das methodische Vorgehen des Forschungsdesigns aufgestellt und Themenpunkte, wie die Unterschiede zwischen qualitativer und quantitativer Forschung gegenübergestellt. Die im Rahmen der qualitativen Forschung verwendeten Experteninterviews werden erklärt sowie das Vorgehen der Akquirierung der Interviews, der Aufbau des

Gesprächsleitfadens dargestellt und über den Durchführungszeitraum sowie die Dokumentationsform informiert.

Fortführend werden im siebten Kapitel die gewonnenen Erkenntnisse auf Basis der Experteninterviews und Auswertung ausgeführt. Abschließend werden die Ergebnisse diskutiert und ein Ausblick auf weiterführende Forschungsthemen gegeben.

1.4 Methodisches Vorgehen

Um die zuvor vorgestellte Forschungsfrage beantworten zu können, werden wissenschaftliche Methoden zur empirischen Untersuchung auf ihre Vor- und Nachteile untersucht und ausgewählt. Darauffolgend werden die zuvor aufgestellte Hypothesen auf ihre Richtigkeit überprüft (Raithel, 2008). Die Untersuchungsmethoden der Sozialwissenschaften teilen sich laut Literatur in quantitative (Bortz & Döring, 2006) und qualitative Vorgehen (Misoch, 2015) auf, deren Unterschiede in der Gestaltung, in der wissenschaftlichen Arbeit genauer erklärt werden. Im Rahmen der Arbeit wird eine Untersuchung mit der Methodik der qualitativen Inhaltsanalyse nach Mayring durchgeführt.

Um einen tiefen Experteneinblick in die Thematik zu erhalten, wird eine qualitative Untersuchung ausgewählt, weil sich Expert*innen leicht mobilisieren lassen, eine große Expertise bereithalten sowie über das gewählte Thema gewonnene Erfahrungswerte berichten können (Bogner, Littig & Menz, 2014).

Als Expert*innen werden Personen im IT-Management, Operations, Helpdesk oder vergleichbaren Funktionsbereichen gewählt. Die Expertise in der Planung als auch dem täglichen Arbeiten in diesen Tätigkeitsbereichen sowie deren tiefe Einblicke in potentielle Herausforderungen werden Gegenstand der Untersuchung werden.

2 IT-SERVICE-MANAGEMENT

In diesem Kapitel der vorliegenden Arbeit werden die theoretischen Grundlagen für die Beantwortung der im Abschnitt 1.2 Forschungsziel erläuterten Forschungsfrage dargelegt. Begonnen wird mit der grundlegenden Definition von IT-Service-Management (ITSM) und danach wird diese Erklärung in die branchenüblichen Rahmenwerke übergeleitet. In den definierten Frameworks wird genauer erläutert, wie ITSM abgebildet wird und welche Prozesse bei der Aktivität der Monitorings mitwirken.

2.1 Definition

ITSM ist ein Ansatz, der es einer Organisation ermöglicht, den wirtschaftlichen Nutzen aus dem Einsatz von Informationstechnologie zu maximieren.

ITSM positioniert IT-Services als zentrales Mittel zur Bereitstellung und Generierung von Nutzen, wobei ein interner oder externer IT-Dienstleister mit Organisationen zusammenarbeitet und gleichzeitig die Verantwortung für die damit verbundenen Kosten und Risiken übernimmt. ITSM erstreckt sich über den gesamten Lebenszyklus eines Services, von der ursprünglichen Strategie über das Design, die Realisierung bis hin zum Produktivbetrieb (Axelos, 2021).

Die Zielsetzungen der ITSM ist, die Unternehmensführung in der Erfüllung aller ihr gesetzten Ziele unter Einhaltung der gesetzlichen Regelungen und dem Schutz von Menschen, Umwelt und Kapital zu unterstützen (Beims, 2010). Unter dem Druck der Veränderung der Unternehmensausrichtung aufgrund von sich immer schneller ändernden Marktanforderungen, ist es nötig, die IT des Unternehmens in beratender Funktion einzusetzen um strategische Impulse einzuleiten und neue Möglichkeiten aufzuzeigen (Beims, 2010).

Diese Ziele des IT-Governance werden meist in standardisierter Form eines Frameworks umgesetzt. Die Integration der Modellumsetzungen von IT-Organisationen und deren Leistungen in Form von Prozessen ist eine tiefgreifende Veränderung und bedarf intensiver und vollumfänglicher Planung. Diese Planung setzt die Bewusstmachung des Reifegrads der IT-Organisation voraus, um ein klares Bild über den Stand der Abläufe und die darauffolgenden Änderungen erhalten und einleiten zu können (Beims, 2012). Daraus sollen schließlich Funktionsbereiche der IT-Organisation aufgebrochen werden, um eine effizientere Prozess- und Serviceorientierung erbringen zu können (Martin Andenmatten, 2021).

2.2 IT-Governance

IT-Governance beschreibt die Verantwortung der Führungskräfte und des Vorstands. Sie besteht aus der Führung, den Organisationsstrukturen und den Prozessen, die sicherstellen, dass die IT

des Unternehmens die Strategien und Ziele des Unternehmens unterstützt und erweitert (Brand & Boonen, 2007).

Eine weitere, ausführlichere Beschreibung laut Brand& Boonen ist wie folgt:

IT-Governance integriert und institutionalisiert Best Practices für die Planung, Organisation, Beschaffung, Implementierung, Bereitstellung, Unterstützung sowie Überwachung und Analyse der Leistung von angebotenen Services, um sicherzustellen, dass die Informationen des Unternehmens und die damit verbundenen Systeme die Unternehmensziele unterstützen. IT-Governance versetzt das Unternehmen in die Lage, den vollen Nutzen aus seinen Informationen zu ziehen und so die Vorteile zu maximieren und Chancen zu nutzen, um einen Wettbewerbsvorteil zu erzielen (Brand & Boonen, 2007).

2.3 IT-Performance-Management

Um die IT-Governance gewährleisten zu können, muss auch ein Kontrollprozess parallel ausgeführt werden. Dieser Prozess, welcher als IT-Performance-Management beschrieben wird, kann in folgende Teilbereiche aufgeteilt werden: (Buchta, Eul & Schulte-Croonenberg, 2010)

- Kosten
- Performance

Im Rahmen dieser Arbeit wird hauptsächlich der Performancebereich betrachtet. Das Ziel des Performance-Managements einer IT-Organisation ist es, zu jedem Zeitpunkt volle Informationen zum Status und der Funktionsfähigkeit der bereitgestellten Services hat (Buchta et al., 2010). Der Hintergrund des IT-Performance-Managements im Rahmen des Controlling Prozesses ist die Rolle der IT als Wertsteigerer. Diese Funktion kann nur erfüllt werden, wenn IT Systeme, welche zur Optimierung von Businessprozessen in Form von Kosteneinsparungen, Verbesserungen der Prozessdurchführung oder Prozesserweiterung beitragen, diesen Beitrag auch kontrollierbar unterstützen (Buchta et al., 2010).

Ziel von IT-Performance-Management ist es, die laufenden Prozesse durch kontinuierliche und - soweit möglich - automatisierte Messung und Analyse einer ständigen Verbesserung zu unterziehen. Key-Performance-Indikatoren dienen somit als Basis für den nachhaltigen Erfolg des Systems. Performance-Management und Prozesscontrolling werden zusätzlich zu einem wichtigen Bestandteil des unternehmensweiten Controllings (Scheer, 2006).

Einige Herausforderungen, wie in der Literatur von Buchta et al. beschrieben, sind: (Buchta et al., 2010)

- Es war schwierig, die Umsetzung der IT-Strategien zu steuern und zu überwachen.

- Es gab keine gemeinsame Basis für konzernweites Leistungsvergleich oder den systematischen Austausch von Best Practices.
- Die CIOs standen unter Budgetdruck, da sie die IT-Leistung nicht ausreichend transparent darstellen und entsprechend kommunizieren konnten.

Um diesen Problemen entgegenzutreten, bietet es sich an die Checkliste aus Tabelle 1 durchzugehen um sich mit den aktuellen Unstimmigkeiten in der Umsetzung zu konfrontieren: (Buchta et al., 2010)

Steigert das IT-Performance-Management-System Ihres Unternehmens die Wertschöpfung durch IT?	
Wird die Umsetzung der IT-Strategie quantifizierbar gemacht?	
Gibt es eine systematische und strukturierte Basis für die interne und externe Kommunikation zwischen Geschäftsbereichen und Anwendern?	
Sind die Maßnahmen zur Zielerreichung in Form von Zielen und KPIs festgelegt und gemessen?	
Tauschen die Geschäftsbereiche Erfahrungen über Best Practices aus?	
Können die Services leicht mit internem und externem Leistungsvergleich gemessen werden, um festzustellen, in welchen Bereichen die Leistung verbessert werden könnte?	
Gibt es in den IT-Projekten eine klare Trennung der Verantwortungsbereiche für Kosten und Services zwischen Projektleitern und Verantwortlichen für den Betrieb?	
Gibt es eine ausreichende Kommunikation zwischen den Verantwortlichen für das IT-Performance-Management, den Verantwortlichen für den Betrieb und den Projektleitern?	

Tabelle 1: Checkliste für IT-Performance-Management

2.4 IT-Ziele

Ein Eckpfeiler des IT-Performance-Managements ist es Dinge (in diesem Kontext die angebotenen Services der IT) mittels festgelegter Ziele messbar zu machen. Der Grundgedanke die Performance von erbrachten Leistungen messbar zu machen, ist es einerseits den Erfolg der Erbringung zu messen (Wird Service A in ausreichendem Maße, also wie für die Durchführung der Businessprozesse benötigt, erbracht?) und andererseits, wenn der Service nicht die gesetzten Performanceziele erreicht, wie dieser zur vollständigen Zielerreichung gesteuert werden kann (Beims, 2012).

Das primäre Ziel, laut (Bainey & Kenneth, 2016) ist es, die wichtigsten Aspekte der IT-Zielsetzung hervorzuheben, indem die Vision, Mission, Ziele, Werte, Erfolgsfaktoren und leistungsorientierten Faktoren während des Verwaltungsprozesses, der Messungen, Umsetzung und Verbesserung der IT-Services beschrieben werden. Die IT-Zielsetzung richtet sich nach dem IT-Strategieframework und dem IT-Service-Lifecycle. Sie wird mit dem Performance-Management-Plan gemessen und mit dem IT-Betriebsplan umgesetzt. Die integrativen Eigenschaften der IT-Zielerklärung mit dem IT-Strategierahmen, dem integrierten System zur Messung der IT-Leistung und den strategischen IT-Richtlinien bieten den Rahmen, um die Nutzung der Ressourcen zu optimieren und die organisatorische Leistung zu verbessern. Führungskräfte sollen die IT-Zielerklärung als Grundlage der Kommunikation, Integration und für das Treffen von faktengestützten strategischen und operativen Entscheidungen nutzen. Strategische Managemententscheidungen sollten auf Grundlage objektiver Beurteilungen und unter Berücksichtigung der betrieblichen Auswirkungen getroffen werden und nicht auf Grundlage von Emotionen, die auf potentiell eigennützigen politischen Agenden basieren. Fundierte objektive Urteile

Entscheidungen erfordern ein Verständnis der Geschäftsleitung für Vision, Mission, Ziele, Werte und Erfolgsfaktoren sowie ein Verständnis für die integrierten Komponenten zur Verbesserung der Qualität des Managements und der gesamten IT-Leistung.

Um einen maximalen Nutzen aus dem Performancemonitoring zu generieren, ist es essenziell die IT-Ziele nicht als Selbstzweck zu definieren, sondern diese mit den Unternehmenszielen in Einklang zu bringen (siehe Abbildung 1). Eine derartige Ausrichtung trägt dazu bei, die enge Abstimmung der von der IT unterstützten Organisation aufrechtzuerhalten (Beims, 2012).

Ein Best Practice zur allgemeinen Zieldefinition lautet die Formulierung SMART, welches im Englischen für ***S**pecific **M**easurable **A**chievable **R**easonable **T**ime-Bound* steht und ein Unternehmensweit konsistentes IT-Rahmenwerk zu verwenden. Auf beide der erwähnten Themen wird in den folgenden Abschnitten noch eine ausführliche Definition Rahmenwerke und Ausschnitte im Bezug zu IT-Governance dargelegt.

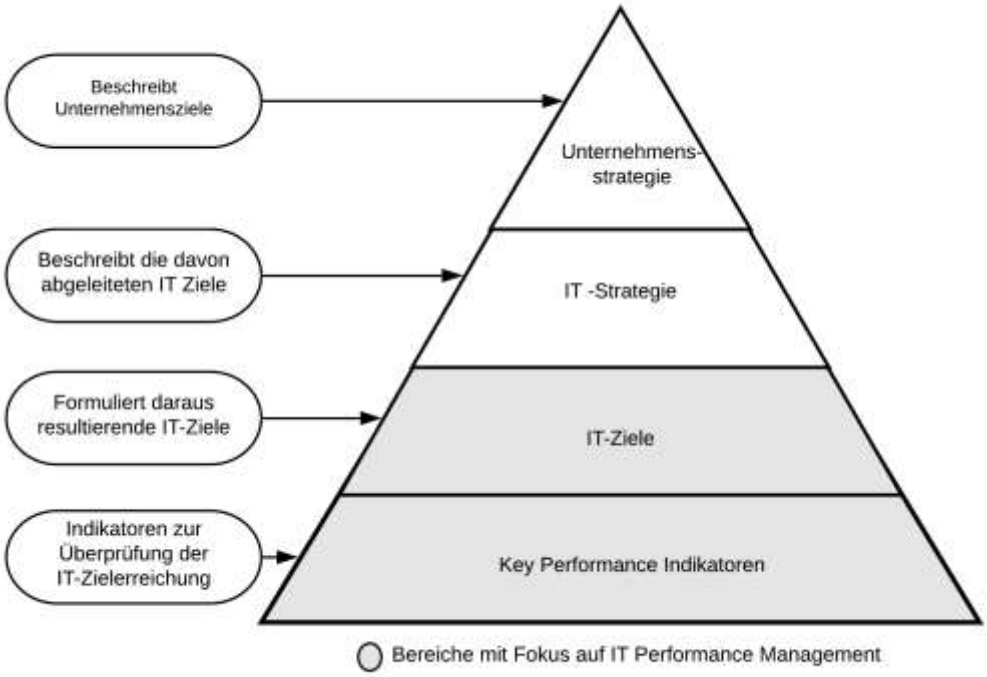

Abbildung 1: Ableitung von Unternehmenszielen bis zu KPIs (in Anlehnung an Buchta et al., 2010)

2.5 Key-Performance-Indikatoren

Auf Basis der IT-Ziele, werden in diesem Abschnitt Key-Performance-Indikatoren (KPI) beschrieben. KPI unterstützen die Fortschrittsermittlung von festgelegten Kennzahlen und weisen auf mögliche Handlungsoptionen hin. Diese speziellen Kennzahlen dienen zur Überprüfung (beziehungsweise dem Controlling) von Prozessen (im Kontext dieser Arbeit werden Services betrachtet) und deren Leistung sowie Auslastung (Gabler Wirtschaftslexikon, 2018). Ableitend aus der Leistungsmessung von Prozessen, kann somit auch festgestellt werden, ob Leistung in ausreichendem Maße (für Zielerreichung) erbracht wird.

Um die Zuordnung von KPIs zu den zugehörigen Zielen zu erleichtern, hilft es eine weitere Zwischenebene (siehe Abbildung) einzubauen. Diese Ebene nennt sich Critical-Success-Factors (CSF). CSF sind Erfolgsfaktoren zur Erreichung der definierten Ziele. Ein Ziel hat mindestens einen CSF (siehe Abbildung 2), in den meisten Fällen jedoch mehrere. Die Wahrscheinlichkeit der erfolgreichen Zielerfüllung steigt mit steigt mit der Erfüllung der CSF (Beims, 2012).

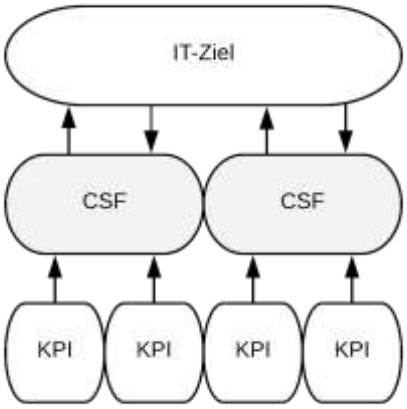

Abbildung 2: Einführung von CSF als Zwischenebene bei KPI und Zielen (in Anlehnung an Beims, 2012)

Da die Entwicklung passender Kennzahlen für die individuellen Ziele große Aufwände mit sich zieht, wird diese Tätigkeit oft unterschätzt. Je nach Ziel der Messung, kann beispielsweise die Servicequalität der Problemlösung anhand der Dauer bis zum Abschluss der Lösungstätigkeit erhoben werden. Die Abgrenzung der Inbegriffenen Teilbereichen und Tätigkeiten ist jedoch sehr komplex, und muss daher im Vorhinein ausführlich abgesteckt und diskutiert werden. Dadurch wäre es im oben erwähnten Fall der Problemlösung sinnvoll, dass die Dauer ab Beginn der Ticketeröffnung bis zum Abschluss und Abnahme des Ticket erfolgt (Beims, 2012).

2.6 Rolle des Continual-Service-Improvement

Continual-Service-Improvement (CSI) findet in allen Bereichen der Organisation und auf allen Ebenen statt, von der strategischen bis zur operativen Ebene. Um die Effektivität von Dienstleistungen zu maximieren, sollte jede Person, die zur Erbringung einer Dienstleistung beiträgt, das CSI im Auge behalten und stets nach Verbesserungsmöglichkeiten suchen. Die prozedurale Darstellung mit den dazugehörigen Outputs der Schritte wird in Abbildung 3 dargestellt.

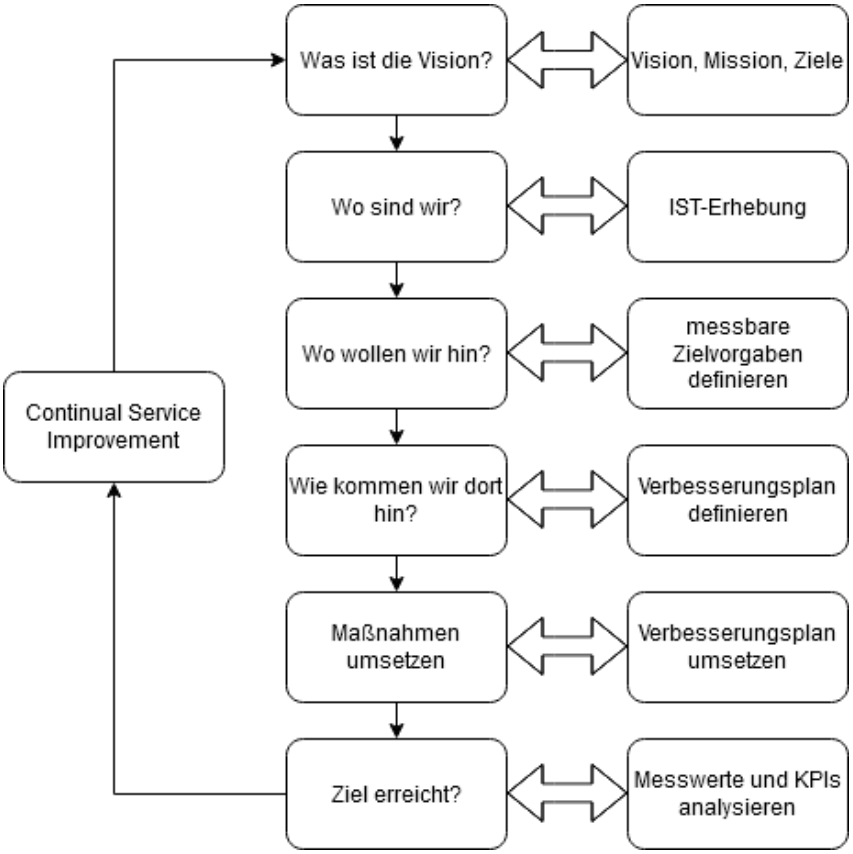

Abbildung 3: Darstellung des Continual-Service-Improvement Prozess (in Anlehnung an Axelos, 2019)

2.6.1 PDCA-Zyklus

Der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) aus dem Qualitätsmanagement eignet sich auch um KPIs auf ihre Qualität hin zu prüfen und verbessern (siehe Abbildung 4) (Beims, 2012). Die Phasen den PDCA-Zyklus sind: (REFA Group, 2021)

- Plan
    - Planungsprozess welche Zieldefinition behandelt, Maßnahmen festlegt, Rollen und Verantwortlichkeiten identifiziert. Erst mit der Ermittlung des IST-Zustands kann die Richtung, also das Ziel festgelegt werden.
- Do
    - Die zuvor festgelegten Maßnahmen werden in diesem Schritt umgesetzt und relevante Informationen festgehalten.
- Check
    - Behandelt die Messung der relevanten Daten zur Zielerfüllung. Es wird beurteilt, inwieweit die zuvor festgelegten Ziele erreicht worden sind.
- Act
    - Analyse von Abweichungen der geplanten Ziele sowie Bewertung dieser, inklusive Maßnahmen zur Korrektur der Zielerreichung für den nächsten Durchlauf des

PDCA-Zyklus. Zudem wird der Standardprozess nach Optimierung der Abweichungen festgelegt, welcher als zukünftige Orientierung dient.

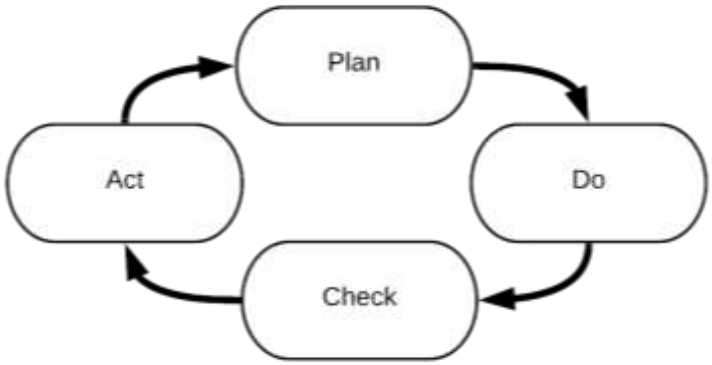

Abbildung 4: PDCA-Zyklus (in Anlehnung an Beims, 2012)

2.6.2 7-Step-Improvement-Prozess

In diesem Abschnitt wird der 7-Step-Improvement-Prozess (siehe Abbildung 5) dargestellt und auf dessen Ziele sowie Integration in den PDCA-Zyklus genauer eingegangen. Dieser wird durchgeführt, um kontinuierlich die Leistungsfähigkeit eines Service zu evaluieren und bei Schwachstellen der Anforderungserfüllung darauf zu reagieren. Die kontrollierte Evaluierung hilft dabei, Messdaten zu definieren und abzuleiten, Messkriterien und Methoden zu finden, zu implementieren und Entscheidungen auf Basis der verdichteten Ergebnisse zu treffen (Beims, 2012).

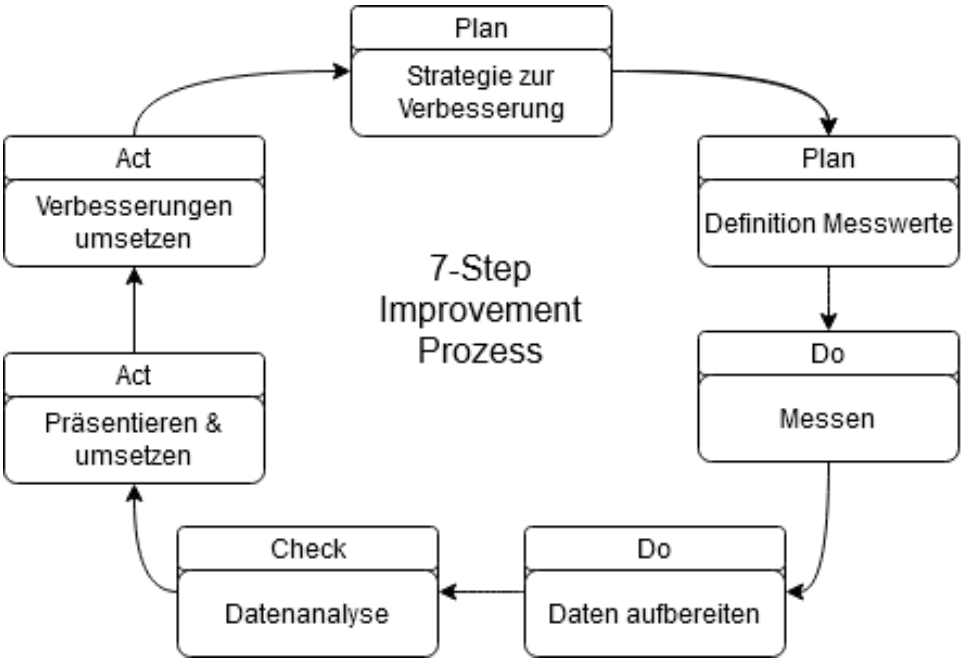

Abbildung 5: 7-Step-Improvement-Prozess (in Anlehnung an Beims, 2012)

Die Schritte des dargelegten Prozesses gliedern sich wie folgt in die Schritte des PDCA-Zyklus und vereinen in den Teilschritten folgende Aufgaben:

- Plan
    - Strategie zur Verbesserung
        - Findung und in Beziehung setzen folgender Einflussfaktoren
            - Vision und Mission Statement
            - Unternehmensanforderungen und Vorgaben
            - Unternehmensstrategie
            - Strategische sowie taktische Ziele
            - Operative Ziele und Verfahren
    - Definition der Messwerte
        - Aufbauend auf den zuvor bestimmten Einflussfaktoren wird in diesem Schritt festgelegt welche Messwerte definiert werden, um die Zielerreichung überprüfen zu können. Hierbei gibt es wichtige Informationen, welchen erheblichen Einfluss haben können. Ein häufiger Fehler ist jedoch, zu viele Kennzahlen zu definieren und folglich den Überblick zu verlieren. Hinderlich kann zudem der Aufwand der Kennzahlenerfassung sein, da dieser unter Umständen zu umfangreich werden kann (beispielsweise, wenn Aufwand häufigen manuellen Erfassung nicht vertretbar mit dem Nutzen ist).
            - Vision und Mission Statement
            - Service-Level-Requirements und Ziele
            - Unternehmensziele, Bereichsziele und IT-Ziele
            - Anforderungen aus Regulatorien und Gesetzgebern
            - Balanced Scorecard
- Do
    - Messen
        - Die Aufgabe dieses Schrittes ist das Erheben der definierten Messwerte. Es werden Informationen zu Services, Prozessen oder Configuration-Items (CI) aufgezeichnet. Im Laufe des CSI können sich die Rahmenbedingungen (Messwerte und Anforderungen) ändern, daher passt sich in diesem Schritt laufend der Output (also die erhobenen Messwerte) an. Die Kommunikation der Änderungen bei den Anforderungen bedarf einer Schnittstelle aus dem CSI. Um diesen Schritt kontrolliert durchführen zu können, benötigt es folgende Informationen:

- Verantwortlichkeit der Monitoring Aktivität
- Zuständigkeit der Monitoring Aktivität
- Frequenz der Monitoring Aktivität
- Integrität der Messwerte

▪ Zu beachten gilt es, die Messwerte in drei verschiedene Kategorien zu unterteilen:

- Technologische-Kennzahlen
  - Infrastruktur, Anwendungen
  - Reaktionszeit, Auslastung, Verfügbarkeit, Antwortzeiten und weitere
- Prozess-Kennzahlen
  - CSF und KPI siehe Abschnitt 2.5
  - Prozesseffektivität, Effizienz und Compliance
- Service-Kennzahlen
  - Unter Annahme der Kund*innensicht gemessene Daten (End-to-End-Messung)

o Daten aufbereiten

▪ Hier werden die zuvor erhobenen Daten verdichtet und gruppiert, um die benötigten Informationen abzuleiten. Messwerte verschiedener abhängiger Komponenten (zum Beispiel: Server, Netzwerk, Storage) werden verknüpft um das Big Picture, also das, was bei Kund*innen ankommt, zu erhalten.

- Check

o Datenanalyse

▪ Im fünften Schritt werden die gewonnen und verdichteten Informationen analysiert und ausgewertet. Darauffolgend werden diese in den Kontext mit den zu erreichenden Zielen gesetzt. Diese Analyse erfordert manuelle Arbeit, im Gegensatz zur Aufbereitung aus dem vorangegangenen Schritt, welcher in weitem Maße mit Hilfsmittel automatisiert werden kann. Folgende Fragestellungen sollten während der Erarbeitung der Datenanalyse behandelt werden:

- Sind Trends erkennbar?
- Handelt es sich bei den Ergebnissen um die der Planung?
- Werden die gesetzten Ziele erreicht?

- Sind, laut aktueller Datenlage, zusätzliche Maßnahmen zur Zielerreichung erforderlich?
- Entstehen Kosten aus Zielabweichungen?

  - Präsentieren & Umsetzen
    - Im vorletzten Schritt des Verbesserungsprozesses, werden den Stakeholdern die gewonnen Erkenntnisse präsentiert und davon abgeleitete Maßnahmen vorgeschlagen, um eine etwaige Zielabweichung zu korrigieren

- Act
  - Verbesserungen umsetzen
    - Im letzten Schritt wird nach Genehmigung der Korrekturmaßnahmen, falls nötig, die Umsetzung dieser durchgeführt. Zusätzlich wird der Ausgangspunkt, um die gesetzte Maßnahme, adaptiert und somit für die neue Iteration als neuer Standard gesetzt.

2.6.3 Beispieldefinition IT-Service

Auf Basis der zuvor genannten Eigenschaften und Details, wird in diesem Abschnitt beispielhaft ein IT-Ziel beschrieben. Diese Vorlage, welcher in Tabelle 2 angeführt ist, dient zur Veranschaulichung der Strukturierung und Zieldefinition.

IT-Ziel	Hohe Zufriedenheit mit Reaktionszeiten des Service Desk
KPI	Kundenzufriedenheit bei Reaktionszeit
Zielwert	2
Verantwortlicher	Leiter*in Service Desk
Messdaten für Zielerreichung	***Verantwortlicher***
Proaktive Messungen	
• Befragungssystem zur Zufriedenheit	Service Desk
• Kundenanalyse durchführen	
Reaktive Messungen	Leiter*in Service Desk
• Kundenkommunikation verbessern	

Tabelle 2:Beispieldefinition IT-Ziel (in Anlehnung an Buchta et al., 2010)

2.6.4 Service-Level-Management

Der Zweck der Service-Level-Management-Praxis ist es, klare unternehmensbezogene Ziele für Service-Levels festzulegen und sicherzustellen, dass die Erbringung von Dienstleistungen adäquat gemessen, überwacht und anhand dieser Ziele gesteuert wird. Die Aufgaben und Ziele des Service-Level-Managements (SLM): (Axelos, 2019)

- schafft eine gemeinsame Übersicht über die Services und erwarteten Service-Levels mit den Kund*innen
- stellt sicher, dass die Organisation die definierten Service-Levels durch die Sammlung, Analyse, Speicherung und Berichterstattung der relevanten Metriken für die identifizierten Services erfüllt
- führt Service-Reviews durch, um sicherzustellen, dass der aktuelle Leistungsumfang weiterhin die Anforderungen der Organisation und ihrer Kund*innen erfüllt
- und berichtet über Service Probleme, einschließlich der Leistung gegenüber den definierten Service-Levels

Der Fokus des SLM sollte ableitend von diesen Zielen daher folgendes sein: (Axelos, 2019)

- Die Einbindung Servicebeziehers ist notwendig, um die tatsächlichen laufenden Bedürfnisse und Anforderungen zu verstehen und zu bestätigen, nicht einfach das, was vom Dienstleister aufgefasst, oder mehrere Jahre zuvor vereinbart wurde.
- Hinhören ist wichtig als beziehungs- und vertrauensbildende Maßnahme, um Kund*innen zu zeigen, dass sie wertgeschätzt und verstanden werden. Dies trägt dazu bei, dass sich der Anbieter nicht immer im Problemlösungsmodus befindet, sondern eine neue, konstruktivere Partnerschaft aufbauen kann.

Zudem muss sich das SLM um das Sammeln und Analysieren von Informationen aus unterschiedlichsten Quellen kümmern, um den*die Kund*in und dessen*deren Anforderungen wirklich auffassen zu können. Diese lauten: (Axelos, 2019)

- Kundenengagement
- Kundenfeedback
- Operative Kennzahlen
- Betriebskennzahlen

2.6.5 Service-Level-Agreements

Service-Level-Agreements definieren die Rahmenbedingungen zur Erbringung von Services. Ziel ist es, die vom*von Kund*innen erwartete Qualität (in diesem Kontext bedeutet dies, dass der Service in ausreichender Menge und Güte zur richtigen Zeit am richtigen Ort zur Verfügung steht) eines in Anspruch genommenen Services in definiertem Maß zu liefern. Zusätzlich dienen vertraglich festgelegte Serviceeigenschaften zur rechtlichen Absicherung, da beide

Vertragsparteien vor der Inanspruchnahme über diese informiert sind (Schiefer & Schitterer, 2008). Anforderungen an solch eine Vereinbarung sind: (Axelos, 2019)

- Es muss sich auf einen definierten Service im Servicekatalog beziehen, andernfalls handelt es sich schlicht um zweckfreie Kennzahl, welche keine ausreichende Aussagekraft bieten oder die Servicequalität nicht widerspiegelt.
- Sie sollten sich auf definierte Ergebnisse beziehen und nicht nur operative Metriken sein. Eine ausgewogene Kombination von Metriken kann dies erreichen, zum Beispiel Kundenzufriedenheit und wichtige Kennzahlen.
- Sie sollten eine Vereinbarung widerspiegeln, das bedeutet einen Dialog und eine Abstimmung zwischen dem Serviceanbieter und dem*der Servicekund*in (Customer). Es ist wichtig, alle Stakeholder einzubeziehen, einschließlich Partner, Geldgeber*innen, Anwender*innen und Kund*innen.
- Sie müssen einfach geschrieben und für alle Parteien leicht zu verstehen und verwenden sein.

Des Weiteren sollte ein SLA folgende Rahmenbedingungen beschreiben und für beide Vertragsparteien deren Pflichten darzustellen: (Beims, 2012)

- Vertragspartner sowie deren Unterschriften
    - Dient zur förmlichen Bestätigung der Zusage zu den genannten Bedingungen
- Servicebeschreibung
- Servicezeiten
- Verfügbarkeit
- Zuverlässigkeit
- Supportvereinbarungen
- Performance
- Weiterführungsmodalitäten des Services im Falle eines weitreichenden Desasterfalls (Service Continuity)
- Security Maßnahmen
- Verantwortlichkeiten
- Preismodell
- Reporting

Weiterführend ist eine übliche Vorgehensweise, SLAs auf Kund*innen oder Services selbst abzustimmen. Diese Varianten nennen sich **Kundenbasierende SLA, Servicebasierende SLA** und **Multilevel SLAs**.

Kundenbasierende SLAs werden für Endkund*innen präferiert herangezogen, um in einem Vertragsdokument alle genutzten IT-Services abzudecken, mit der Auswirkung, dass weniger administrativen Aufwand für den Umgang mit Dokumenten erzeugt wird.

Sollten diese Dokumente für eine ganze Kundengruppe angewendet werden, hat es zur Folge, dass nicht auf individuelle Kundenanforderungen innerhalb der gleichen Kundengruppe eingegangen werden kann (Beims, 2012).

Servicebasierende SLAs sind unspezifischer auf Kund*innen gestaltet, da sie grundsätzlich dazu dienen alle Bezieher*innen eines einzelnen Service zu bedienen. Im Kontrast zu kundenbasierten SLAs, liegt hier der verringerte administrative Aufwand beim Serviceanbieter. Daraus ergibt sich die Tatsache, dass nur ein Dokument für den Service entworfen wird, und nicht viele kundenbasierten SLAs in Einklang gebracht werden müssen. Hierbei stehen viele Kunden*innen mit einzelnen, gleichen Services aber mit unterschiedlichen Anforderungen an in Beziehung. Dies ist jedoch auch gleichzeitig der Nachteil, da individuelle Kundenanforderungen nicht berücksichtigt werden können, da eine einzelne Lösung für alle angeboten wird (Beims, 2012).

Multilevel SLAs werden Verträge genannt, welche eine Kombination aus verschiedenen Vereinbarungsebenen darstellen. Sie bilden alle konzernweiten Servicevereinbarungen als Rahmenbedingungen ab und werden in drei Stufen unterteilt. Diese sind die Konzernebene, Kundeneben und Serviceebene. Der Detailgrad erhöht sich je tiefer in die Kunden- und Serviceebene vorgedrungen wird, und verringert sich bei der allgemein gehaltenen Konzernebene (Beims, 2012).

2.6.6 Operational-Level-Agreements

Operational-Level-Agreements (OLA) regeln Vereinbarungen zur organisationsinternen Leistungserbringung. Meist werden SLAs OLAs vorangestellt (wie in Abbildung 6), um kritische Zwischenziele für die externe Leistungserbringung gewährleisten zu können (Beims, 2012).

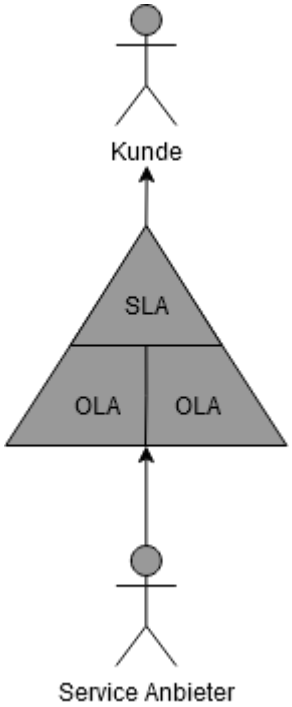

Abbildung 6: Verhältnis von SLA, OLA, Kunde und Service Provider

2.6.7 Balanced Scorecard

Mittels der Balanced Scorecard als Managementsystem werden Vision und Strategie in Aktionen überführt. Die Balanced Scorecard durchzieht alle Unternehmensbereiche und deklariert die IT-Prozesse als Support-Prozesse zur Erfüllung der Unternehmung selbst. In Kooperation mit der Unternehmensleitung wird eine auf die Vision und Ziele abgestimmte Scorecard erstellt (Goltsche, 2006).

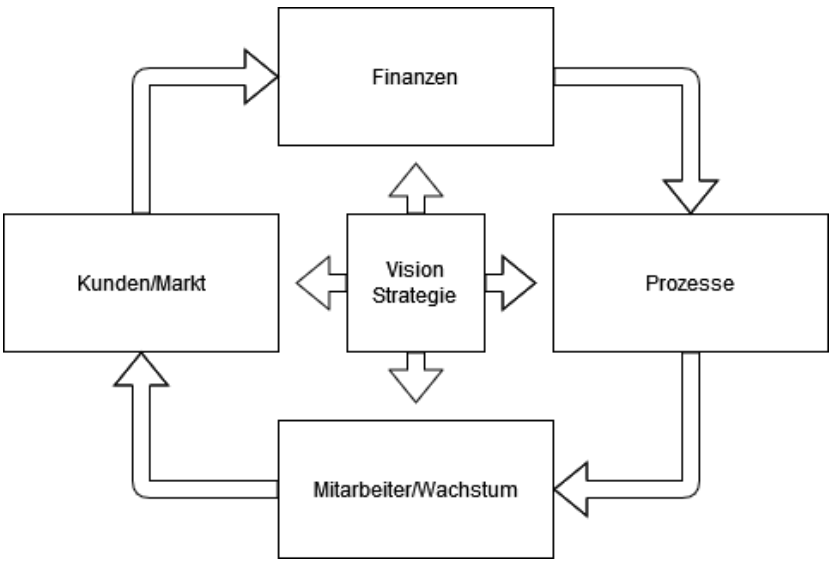

Abbildung 7: Balanced Scorecard Modell (in Anlehnung an Goltsche, 2006)

2.7 Rahmenwerke der IT

Aufgrund des Umfangs der Rahmenwerke werden nur relevante Teilbereiche des ITSM, IT-Governance und IT-Performance-Management in nachfolgenden Abschnitten beleuchtet.

2.8 ITIL

Als Teil dieser Literaturrecherche wird Information Technology Infrastructure Library (ITIL) näher betrachtet. Dies hat den Hintergrund, dass ITIL als Branchenstandard gilt und die Dokumentation sowie Prozesslandkarte einsehbar ist. In ITIL werden Abläufe der IT prozessorientiert dargestellt und alle dazugehörigen Ressourcen, Stakeholder und Terminologie näher beschrieben. Das Ziel von ITIL ist es, Best Practices von Prozessen für den Einsatz in der eigenen Organisation beziehungsweise dem eigenen IT-Service-Management zu implementieren um die Serviceerbringung noch enger an die Unternehmensziele zu knüpfen (TOPdesk, 2021).

2.8.1 Service Operation

In diesem ITIL Prozess wird die effektive und effiziente Serviceerbringung sichergestellt. Zudem werden in diesem Prozess Clientanforderungen (in Form von Tickets) bearbeitet und Problemlösungen bereitgestellt. Weiters werden betriebliche Standardaufgaben abgewickelt.

Service Operation wird in nachfolgend aufgezählten Teilprozessen und Funktionen aufgeteilt:

- Event Management
- Incident Management
- Request Fulfilment
- Access Management
- Problem Management
- IT Operations Control
- Facilities Management
- Application Management
- Technical Management

Der Zusammenhang der Teilprozesse ist aus Abbildung 8 zu entnehmen.

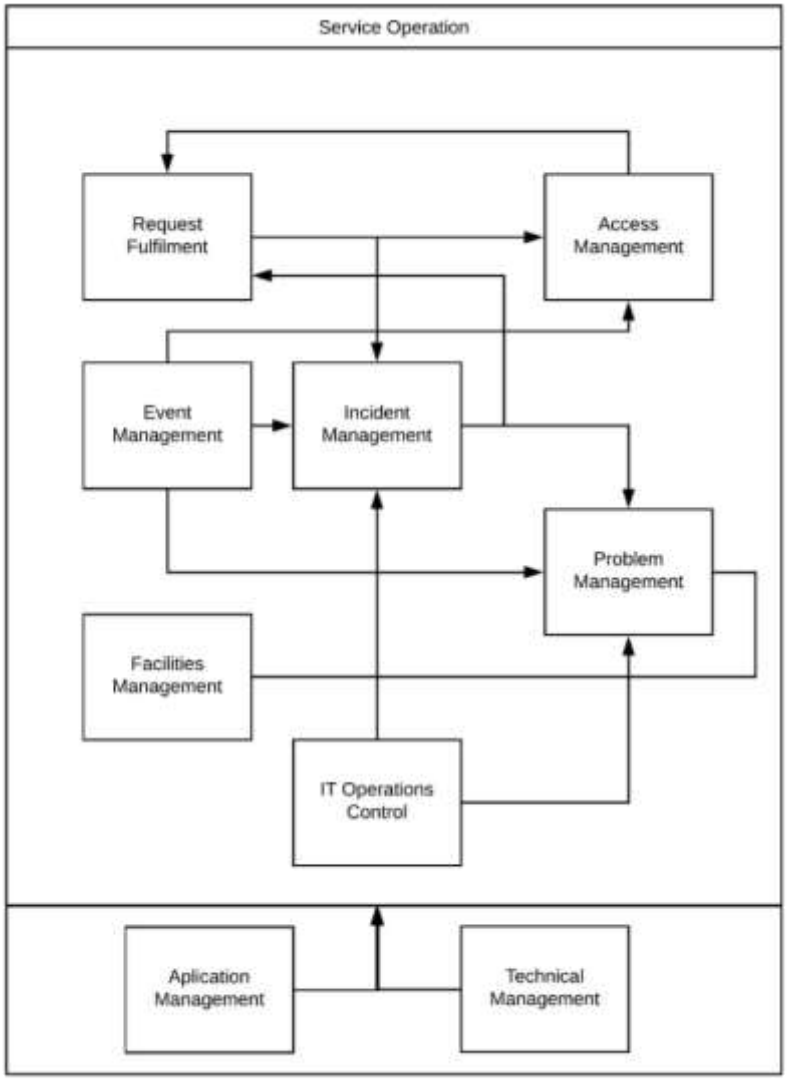

Abbildung 8: ITIL Service Operation Prozess (in Anlehnung an Axelos, 2019)

2.8.2 Rolle des CSI Manager

In ITIL ist der CSI Manager für die Durchführung der Verbesserungsprozesse verantwortlich. Zu seinen essentiellen Funktionen zählen unter anderem: (Beims, 2012)

- Nutzen und Vision des CSI
- Schaffung eines Rollenverständnisses und Zuweisung dieser
- Schnittstelle für Service- und Process Owner im Kontext des CSI
- Management der Monitoringumgebung
- Laufende Adaptierung des Service-Improvement-Plans in Kooperation mit dem Service-Level-Management (SLM)
- Einhaltung der im CSI Plans definierten Aktivitäten im Rahmen des Service Lebenszyklus
- Review der Aktivitäten

- Priorisierung von Maßnahmen aufgrund der individuellen Dringlichkeit und Wichtigkeit
- Reporting an Zielpersonen

2.9 COBIT

In diesem Abschnitt werden das COBIT Modell und die für diese Arbeit relevanten Themenblöcke näher beschrieben.

COBIT, eine Abkürzung für ***C****ontrol* ***Ob****jectives for* ***I****nformation and related* ***T****echnology*, ist ein Kontrollmodell für die gesamtheitliche Abwicklung der IT-Organisation. COBIT dient, wie der Name es schon hinweist, zur Kontrolle beziehungsweise Auditierung der IT. Mithilfe von COBIT werden für die IT-Governance Kontrollziele (englisch: Control Objectives, oder CO) bereitgestellt (Goltsche, 2006). Diese Kontrollmodell wird in Abbildung 9 dargestellt.

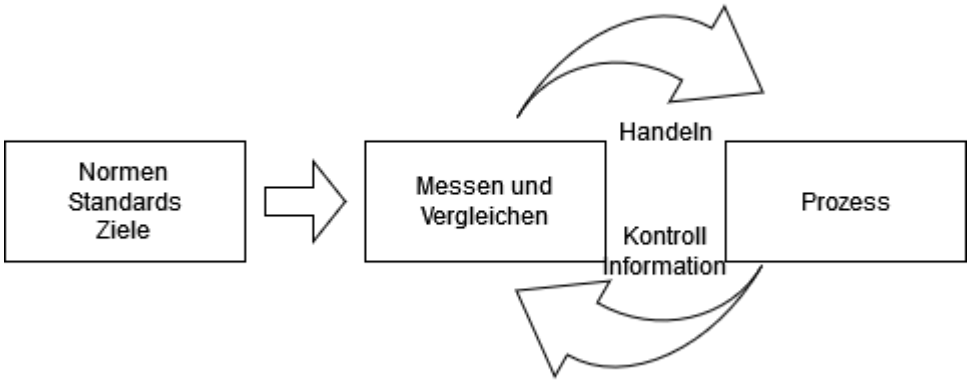

Abbildung 9: COBIT Kontrollmodell (in Anlehnung an Goltsche, 2006)

Für diese Ermittlung der individuell ausgeprägten Reifegrade der Prozesse liefert COBIT prozessbasierte Beschreibungen von Bewertungskriterien. Die Verwendung des Modells ermöglicht es zudem einfacher zu verstehen welche Risiken und Chancen sich bei der Benutzung von unterschiedlichsten Technologien manifestieren können, und wie diese eingeschätzt und behandelt werden sollen (Goltsche, 2006).

2.9.1 Managen der Qualität

Ziel des Qualitätsmanagements im COBIT Rahmenwerk ist es, die Kundenanforderungen zur Gänze zu erfüllen, als auch die Kosten für die Erbringung der erwünschten Qualität auf ein Minimum zu senken und die Zufriedenheit der Kund*innen zu erfüllen (Goltsche, 2006). Die Aktivitäten im Durchlauf des Qualitätsmanagementprozesses sind in Abbildung 10 dargestellt.

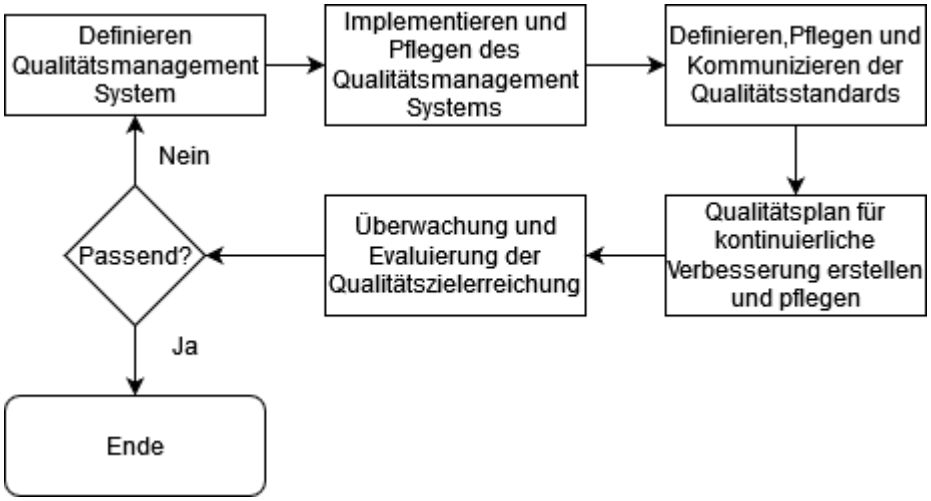

Abbildung 10: Aktivitäten im Qualitätsmanagementprozess (in Anlehnung an Goltsche, 2006)

2.9.2 Überwachen und evaluieren IT Performance

Ob IT-Ziele und Kennzahlen eingehalten werden, erfordert ein kontinuierliches Monitoring und evaluieren. Monitoring sorgt für eine Form der Transparenz in der Einhaltung und Erfüllung definierter Messwerte, welche in einem Anbieter-Kunden Verhältnis definiert wurden. Auf Basis der in der Organisation kommunizierten Kontrollrichtlinien werden Monitoringrichtlinien abgeleitet. In diesen Richtlinien wird festgehalten, auf Basis welcher Kennzahlen der Service über das zu überwachende Objekt gemessen wird (Goltsche, 2006). Diese Kontrollobjekte bauen sich in folgenden Bausteinen auf: (Goltsche, 2006)

- Ziel des Monitorings
- Definition und Prozess, wie Monitoring Daten gesammelt werden
- Darlegung der Art zur Monitoring Daten Aufzeichnung
- Auswertung der Zielerreichung
- Reporting an entscheidende Stellen
- Maßnahmen zur Einhaltung der Ziele

Diese Bausteine werden auch in Abbildung 11 als Prozess dargestellt.

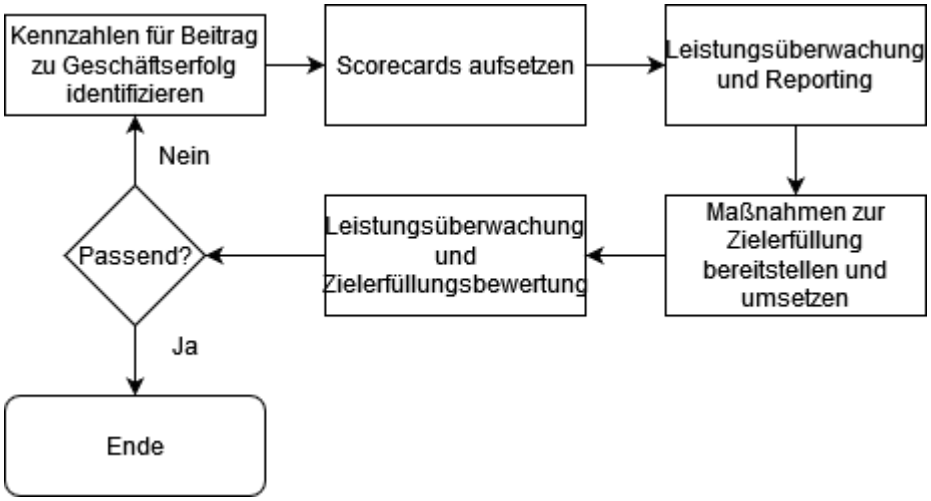

Abbildung 11: Performancemonitoring (in Anlehnung an Goltsche, 2006)

2.10 Prozessreifegradmodell

Das Prozessreifegradmodell mit Fokus auf Softwareentwicklung (englisch auch Capability Maturity Model oder kurz CMM), welches von Softwareentwicklungsinstitut (SEI) der Carnegie Mellon University erstellt wurde, beschreibt wie Organisationen ihre Prozesse basierend auf Stufen optimieren können. Diese Entwicklung, wie in der folgenden Auflistung erläutert, zieht sich von der Entstehung zufälliger Abläufe bis hin zu mit Feedback und Kennzahlen optimierte Prozesse. Die Reifegrade stellen sich wie folgt dar: (Goltsche, 2006)

1. **Initial**
    - Im ersten Reifegrad finden sich chaotische und unkontrollierte Abläufe, welche bedarfsgesteuert abgewickelt werden. Der Prozessoutput hängt von den ausführenden Individuen ab und schwankt dadurch stark in der Qualität.
2. **Wiederholbar**
    - Basierend auf Vorerfahrungen werden im zweiten Reifegrad projektgetriebene Prozesse, deren Kennzahlen zu Kosten, Zeitpläne und Funktionsumfang, umgesetzt. Erfolge aus Erfahrungswerten spielen bei der Prozessabwicklung eine tragende Rolle. Gleichbleibende Abläufe, basierend auf früheren Erfolgen, werden als zielführend angesehen.
3. **Definiert**
    - Im dritten Reifegrad werden organisationsweit Prozesse als Standard definiert, integriert und dokumentiert. Alle Projektprozesse werden auf dem aktuellen Prozessstandard aufgebaut und ausgeführt.
4. **Managed**

- (Produktentwicklungs-)Prozesse werden im vierten Reifegrad quantifiziert und basierend auf den Messergebnissen gesteuert.

5. Optimierung

- Unter Einbindung des PDCA Zyklus (siehe Abschnitt 2.6.1), werden im fünften Reifegrad, Prozesse kontinuierlich verbessert, neue Teilprozesse implementiert und ausgebaut.

Diesem softwareentwicklungsgetriebenen Ansatz steht die branchenunabhängige Herangehensweise des COBIT Modells gegenüber:(Goltsche, 2006)

0. Nicht Existent

- Die Organisation verfolgt keine prozessorientierte Herangehensweise und ist sich des Bedarfs auch nicht bewusst.

1. Initial/ad hoc

- Abläufe werden mit individuellen ad hoc Ansätzen ausgeführt, jedoch entwickelt sich ein Bewusstsein über den Bedarf standardisierter Prozesse. Das Management der IT-Organisation agiert unorganisiert und von Fall zu Fall bedarfsgetrieben.

2. Wiederholbar, aber intuitiv

- Prozesse werden aufgabenorientiert entwickelt und ausgeführt. Eine Standardisierung im Rahmen von Maßnahmen wie Personalschulungen oder zentralisierte Kommunikation zum Vorgehen wird nicht durchgeführt. Die Informationsweitergabe, wie Prozesse abgewickelt werden, obliegt dem Personal selbst. Es wird vermehrt auf Stärken und Erfahrungen der Individuen gesetzt. Die Erfahrungsweitergabe wird nicht forciert. Folglich kommt es zu einem Informationsverlust entlang der aufrührenden Personen.

3. Definierte Prozesse

- Die Standardisierung wird mit Maßnahmen wie Dokumentation und Schulungen des Personals forciert. Die Einhaltung der definierten Prozesse wird jedoch nicht kontrolliert und den Individuen überlassen. Dies führt langfristig zu einer Abweichung der anvisierten Qualität in der Ausführung.

4. Geführt und messbar

- Zur Einhaltung der Rahmenbedingungen werden in dieser Stufe Prozesse und deren Kennzahlen hinsichtlich des Erfüllungsgrads evaluiert. In definierten Abständen werden Prozesse, mittels Maßnahmen hinsichtlich ihrer Effektivität und Effizienz, adaptiert um sie nachhaltig zu verbessern. Dieses Vorgehen bietet eine quantifizierbare Prozesskultur und ermöglicht es Organisationen gleichbleibende Qualität als Prozessoutput zu liefern. Tools und Automatisierungen werden jedoch nur in limitiertem Ausmaß eingesetzt.

5. Optimiert

- Im finalen Reifegrad des COBIT Modells unterliegen Prozesse einem kontinuierlichen Verbesserungsprozess. Diese Herangehensweise und die Betrachtung der IT als Ermöglicher für Prozessautomatisierungen ermöglichen immer weitere und umfangreichere Möglichkeiten Prozesse von Organisationen hinsichtlich ihrer Effizienz zu steigern. Tools werden gezielt eingesetzt und helfen der Organisation, sich auf den ändernden Wettbewerb einzustellen sowie konkurrenzfähig zu bleiben.

2.11 ISO/IEC 20000

In diesem Abschnitt wird genauer auf grundlegende Eckpunkte des Standards ISO/IEC 20000 eingegangen, dessen Hintergründe beleuchtet und Unterteilung dargelegt.

Dieser Standard wurde vom British Standards Institute entwickelt und besteht aus den Teilen ISO/IEC 20000-1:2011 Service Management System Requirements welcher die Spezifikationen der Norm beschreiben, sowie ISO/IEC 20000-2:2005 Code of Practice welcher Empfehlungen zur Umsetzung beinhaltet. Weiters gibt es noch den dritten Teil ISO/IEC 20000-3:2009 Guidance on Scope Definition and Applicability of ISO/IEC 20000-1, mit Ergänzungen der Empfehlungen aus dem zweiten Teil mit Fokus auf der Implementierung eines Service Management Systems, ISO/IEC 20000 Part 4 Process Reference Model als Hilfestellung zur Umsetzung der Norm und ISO/IEC 20000 Part 5 Exemplar Implementation Plan for ISO/IEC 20000-1 mit beispielhafter Umsetzung zur Veranschaulichung. In Abbildung 12 ist die Unterteilung der Norm, beziehungsweise nur dessen Hauptteile 1 und 2, genauer dargestellt sowie Verknüpfungen mit den zuvor beschriebenen Rahmenwerken ITIL und COBIT hergestellt (Beims, 2010).

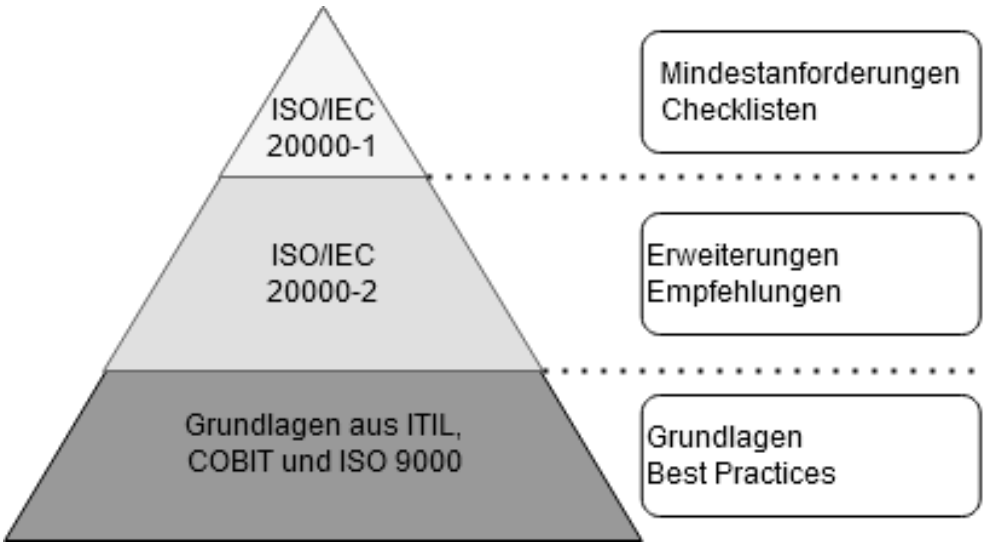

Abbildung 12: Zusammenhang ISO/IEC 20000 und Rahmenwerke für ITSM (in Anlehnung an Beims, 2010)

3 MONITORING

In diesem Kapitel wird der Begriff Monitoring erörtert und welche Themenbereiche daran angeknüpft werden können. Es wird genauer auf Bestandteile von Infrastruktur und Services eingegangen sowie das Thema des Monitorings selbst vertieft. Zudem wird verknüpft welche Teile der IT-Infrastruktur für das ITSM als Basisinfrastruktur gelten und deren Zusammensetzung beschrieben. Weiters wir mit den Knackpunkten des interdisziplinären Monitorings auf Probleme und Lösungen eines komplexen Monitoringkonzepts eingegangen.

3.1 Definition

Im Rahmen der Erfassung und Auswertung von Messgrößen für die Leistung des Qualitätsmanagementsystems muss eine Organisation Informationen darüber sammeln, wie Kund*innen die Erfüllung der Kundenanforderungen wahrnehmen. Die Methoden zur Beschaffung und Verwendung dieser Informationen müssen festgelegt werden (Pierre D. Landry, 2001).

3.2 Infrastruktur

„Als IT-Basisinfrastruktur wird die Menge aller Hardware- und aller systemnahen Softwarekomponenten verstanden, die die Laufzeit- und Managementumgebung für Entwicklung, Test und Produktion von Informationssystemen bilden.“ (Dern, 2009, S. 44)
Diese Beschreibung der IT-Basisinfrastruktur ist in Abbildung 13 dargestellt. Sie wird in die Hauptbestandteile nach Funktionen aufgeteilt, welche Management, Operations und der Security Umgebung in einer Basisplattform umfassen.

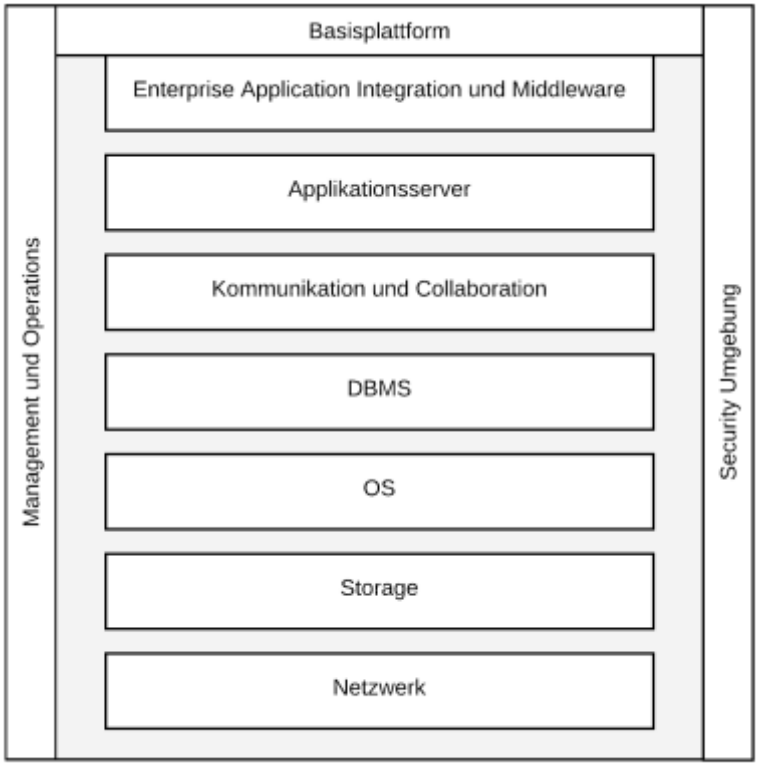

Abbildung 13: Beispielhafte Basisinfrastruktur Darstellung (in Anlehnung an Dern, 2009)

Weiters wird von Rudolph IT-Infrastruktur wie folgt beschrieben:

„Die IT-Infrastruktur umfasst sämtliche Hard- und Software, die zur Verarbeitung, Speicherung und Kommunikation von Geschäftsprozessinformationen eingesetzt wird (technische Infrastruktur). Das umschließt auch Humanressourcen und Dienstleistungen, die zur Installation und Nutzung erforderlich sind (organisatorische Infrastruktur). Diese Bestandteile werden integriert in Form von IT-Services abgebildet, die in ihrer Zusammenstellung den Geschäftsnutzen verdeutlichen und den IT-Nutzern bereitgestellt werden.“ (Rudolph, 2009, S. 14)

3.3 Cloud Service Modelle

Im Abschnitt der Cloud Service Modelle werden verschiedene Ansätze beschrieben, welche es aufgrund des technischen Fortschritts Kund*innen ermöglichen über ein cloudbasiertes Servicemodell unterschiedlichste Bestandteile von IT-Infrastruktur zu beziehen.

Die Bereitstellung, Monitoring und Wartung von Software in der Cloud können sich deutlich davon unterscheiden, wie eine Organisation diese Aufgaben bis zur Implementierung eines Cloud Modells bewältigt. Ob Entwickler*innen, Administrator*innen, Helpdesk-Mitarbeiter*innen und Scrum-Master, diese Personen müssen ein solides Verständnis von Cloud Computing besitzen, um ihren Job in ausreichendem Maße ausführen zu können. Ein breites Wissen über Netzwerke,

Sicherheit, servicebasierte Systeme, Web-Architekturen und vieles mehr ist hierzu essentiell (Kavis, 2014).

3.3.1 IaaS

Ein Teil dieser Cloud Service Modelle ist Infrastructure-as-a-Service (IaaS) und bietet die Möglichkeit, cloudbasierte virtuelle Infrastrukturbestandteile zu beziehen. Dieser Service bietet die Möglichkeit, sich nicht um etwaige Anschaffungskosten, Betrieb oder Hardwareanforderungen für eine Umsetzung kümmern zu müssen. Für die Verwendung von IaaS wird sich nur um die gebuchten Ressourcen gekümmert, welche je nach Verwendung verrechnet werden. Aufgrund dieser einfachen Implementierung ist es auch nötig diesen Teil einer IT-Infrastruktur im Rahmen dieser Arbeit ein besonderes Augenmerk zu widmen (Kavis, 2014).

Das National Institute of Standards and Technology (NIST) definiert IaaS wie folgt:

Die dem Verbraucher zur Verfügung gestellte Möglichkeit besteht in der Bereitstellung von Rechen-, Speicher-, Netz- und anderen grundlegenden Rechenressourcen, auf denen der Verbraucher beliebige Software, einschließlich Betriebssystemen und Anwendungen, einsetzen und ausführen kann. Der Bezieher verwaltet oder kontrolliert die zugrunde liegende Cloud-Infrastruktur nicht, hat aber die Kontrolle über Betriebssysteme, Speicherplatz und bereitgestellte Anwendungen sowie möglicherweise eine begrenzte Kontrolle über ausgewählte Netzkomponenten (z. B. Host-Firewalls) (Mell & Grance, 2011).

Auf Basis der oben erwähnten technischen Möglichkeiten Infrastruktur oder Teile davon über ein Cloud Service Modell abzubilden, ergibt sich folgende Unterteilung wie aus Abbildung 14 zu entnehmen. Darauf aufbauend erschließt sich, dass bei IaaS die Infrastruktur Data Center, Storage, Server, Firewall, Netzwerk und Load Balancer als Service angeboten werden (Kavis, 2014).

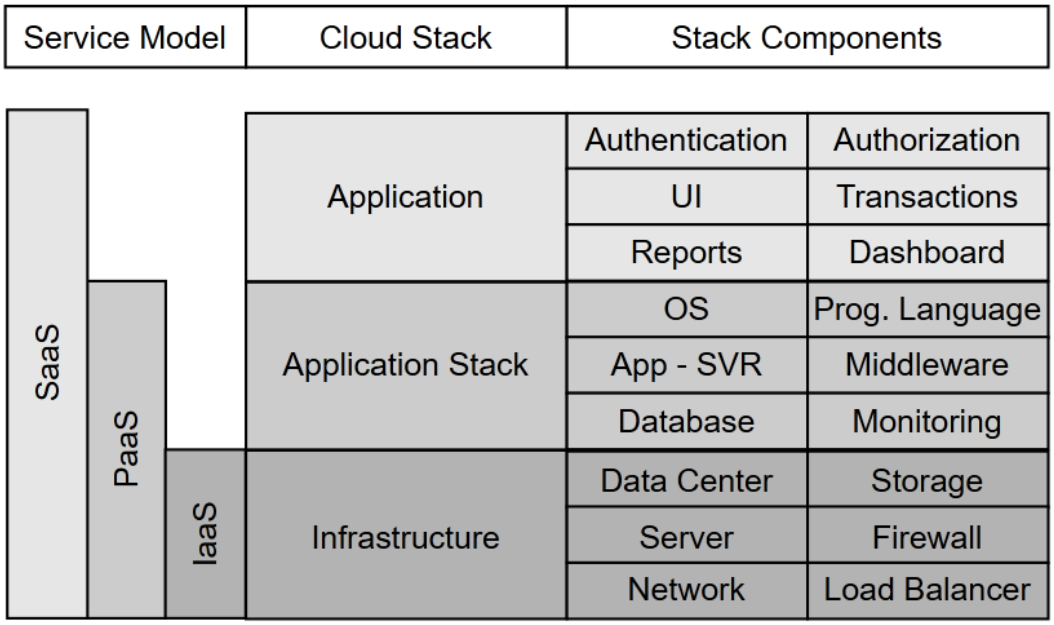

Abbildung 14: Aufteilung von Cloud Modellen (in Anlehnung an Kavis, 2014)

3.3.2 PaaS

Die nächste Stufe auf dem Stack ist PaaS. Was für die Infrastruktur IaaS ist, das ist Platform-as-a-Service (PaaS) für Anwendungen. PaaS setzt auf IaaS auf und abstrahiert einen Großteil der Standardfunktionen auf der Anwendungsebene und bietet diese Funktionen als Service an (Kavis, 2014). Zu diesen vom Anbieter verwalteten Funktionen gehören, wie in Abbildung 14 zu sehen, sind das Betriebssystem (OS), die Programmiersprache der Plattform, Applikationsserver, Middleware, Datenbank und das Monitoring (Kavis, 2014).

PaaS ist die Bereitstellung einer Computing Plattform und eines Solution Stacks als Service. PaaS Angebote erleichtern die Bereitstellung von Anwendungen ohne die Kosten und die Komplexität des Kaufs und der Verwaltung der zugrunde liegenden Hardware und Software sowie der Bereitstellung von Hosting-Funktionen betrachten zu müssen. Damit werden alle erforderlichen Ressourcen bereitgestellt, um den gesamten Lebenszyklus der Entwicklung und Bereitstellung von Webanwendungen und Services vollständig über das Internet zu realisieren (Cloud Security Alliance, 2011).

3.3.3 SaaS

SaaS, gelegentlich auch als On-Demand-Software bezeichnet, ist ein Modell zur Bereitstellung von Software sowie die zugehörigen Daten zentral bereitgestellt werden. Typischerweise werden diese Ressourcen in der Cloud gehostet und von Benutzer*innen über einen Thin Client oder Browser benutzt (Cloud Security Alliance, 2011). Der Serviceprovider ist für die gesamte Infrastruktur, die gesamte Anwendungslogik, alle Bereitstellungsmaßnahmen und allem, was mit der Bereitstellung des Produkts oder der Dienstleistung zusammenhängt verantwortlich (Kavis, 2014) (Cloud Security Alliance, 2011).

3.4 Knackpunkte Interdisziplinäres Monitoring

Themen und Domänenspezifische Werkzeuge für das Monitoring und Auswerten von Performance Kennzahlen sind eine gängige, jedoch nicht zielführende Praxis. Interdisziplinäres Monitoring ermöglicht es, unabhängige Messung von Kennzahlen, ohne von Fachwissen aus nicht passenden Domänen einfließen zu lassen. Ein*e Netzwerkexpert*in hat nicht das passende Wissen um ein Monitoringsystem für Datenbank sachkundig und vollumfänglich aufsetzen oder aktiv betreuen zu können. Jedoch können die Schnittmengen der Fachbereiche sehr wohl großen Einfluss auf die Kennzahlen anderer Bereiche haben. Aus diesem Grund eignet es sich Monitoringsysteme einzusetzen, welche nicht auf Nischen spezialisiert sind, sondern es erlauben die IT einer Organisation und alle dazugehörigen Ressourcen als Ganzes zu betrachten (Jones, 2011).

3.5 Monitoring Tool - System Center Operations Manager

In diesem Abschnitt werden die grundlegenden Funktionalitäten und die Komponenten eines gängigen Monitoring Tools dargelegt. Ein Verständnis über die Funktionsweise eines solchen Werkzeugs soll gebildet werden, da viele der gängigen Lösungen auf ähnliche Weise funktionieren.

Operations Manager, eine Teilkomponente von Microsoft System Center, ist eine Software, mit der sich Dienste, Geräte und Vorgänge für viele Computer von einer einzigen Konsole aus überwachen lassen. Die Verwendung von Operations Manager in der Systemumgebung erleichtert die Überwachung einer Vielzahl von Computern, Geräten, Diensten und Anwendungen. Die Konsole von SCOM ermöglicht es den Zustand, die Leistung und die Verfügbarkeit aller überwachten Objekte in der Umgebung zu überprüfen und hilft, Probleme zu erkennen sowie zu beheben. Organisationen sind in der Regel von den Diensten und Anwendungen abhängig, die von ihrer IT-Umgebung bereitgestellt werden. Die IT-Abteilungen sind dafür verantwortlich, die Leistungsfähigkeit und Verfügbarkeit dieser wichtigen Services und Anwendungen zu gewährleisten. Das bedeutet, dass die IT-Abteilungen erkennen müssen, wenn ein Problem auftritt, dass sie die Ursache des Problems identifizieren müssen und dass die Problemursache herauszufinden ist - im günstigsten Fall, bevor die Anwendungsnutzer die Probleme wahrnehmen. Je mehr Computer und Geräte es in einem Unternehmen gibt, desto herausfordernder wird diese Aufgabe. Operations Manager zeigt auf, welche überwachten Objekte nicht in einem einwandfreien Zustand sind, alarmiert, wenn Probleme festgestellt werden, und liefert Informationen, die helfen die Ursache eines Problems sowie mögliche Lösungen zu bestimmen (Microsoft, 2021).

Bei der Installation von Operations Manager wird eine Managementgruppe eingerichtet. Die Managementgruppe ist die Grundeinheit der Funktionalität. Eine Managementgruppe besteht mindestens aus einem Managementserver, der Datenbank für den Betrieb und der Datenbank für das Reporting Data Warehouse.(Microsoft, 2021)

- Der Managementserver ist der zentrale Punkt für die Verwaltung der Managementgruppen und die Verbindung zur Datenbank. Wenn die Operationskonsole geöffnet und eine Verbindung zu einer Managementgruppen hergestellt wird, wird eine Verbindung zu einem Managementserver für diese Managementgruppe hergestellt. Je nach Größe ihrer IT-Umgebung kann eine Managementgruppe einen einzelnen Managementserver oder mehrere Managementserver enthalten(Microsoft, 2021).
- Die operative Datenbank ist eine SQL-Server-Datenbank, die alle Konfigurationsdaten für die Verwaltungsgruppe enthält und alle Monitoring Daten speichert, welche für die Verwaltungsgruppe gesammelt und verarbeitet werden. Die operative Datenbank speichert kurzfristige Daten, standardmäßig sieben Tage.
- Die Data Warehouse-Datenbank ist eine SQL-Server-Datenbank, in der Überwachungs- und Alarmierungsdaten für historische Zwecke gespeichert werden. Daten, die in die Operations Manager-Datenbank geschrieben werden, werden auch in die Data

Warehouse-Datenbank geschrieben, so dass die Berichte immer aktuelle Daten enthalten. In der Data-Warehouse-Datenbank werden langfristige Daten aufbewahrt.

Managementserver

Die Aufgabe des Managementservers umfasst die Verwaltung der Konfiguration der Managementgruppe, die Verwaltung und Kommunikation mit den (Client-)Agenten sowie die Kommunikation mit den Datenbanken der Managementgruppe.

Die Managementgruppe kann mehrere Managementserver beinhalten, um die Kapazität zu erweitern und eine kontinuierliche Verfügbarkeit gewährleisten zu können. Wenn zwei oder mehr Managementserver zu einer Managementgruppe hinzugefügt werden, werden die Managementserver Teil eines Ressourcenpools und die Arbeit wird auf die Mitglieder des Pools verteilt. Fällt ein Mitglied des Ressourcenpools aus, übernehmen andere Mitglieder die Aufgaben des betroffenen Mitglieds. Wird ein neuer Managementserver hinzugefügt, übernimmt der neue Managementserver automatisch einen Teil der Arbeit der bestehenden Mitglieder des Ressourcenpools. Alle Mitglieder des Ressourcenpools verwalten eine bestimmte Gruppe von Objekten. Zwei Mitglieder desselben Pools können niemals dasselbe Objekt zur gleichen Zeit verwalten(Microsoft, 2021).

(Client-)Agenten

Der Operations Manager Agent ist ein auf dem jeweiligen System installierter Dienst. Der Agent sammelt Daten, vergleicht die gesammelten Daten mit definierten Kennzahlen, erstellt Warnungen und führt Gegenmaßnahmen durch. Ein Managementserver empfängt und verteilt Konfigurationen an Agenten auf überwachten Computern.

Jeder Agent berichtet an einen Managementserver in der Managementgruppe. Dieser Managementserver wird als der primäre Server des Agenten definiert.

Die Agenten überwachen die Datenquellen auf dem zu überwachenden System und sammeln Informationen entsprechend der jeweiligen Konfiguration, welche sie von ihrem Managementserver erhalten haben (siehe Abbildung 15 für Prozess zur Erkennung und Monitoring von Systemen). Der Agent analysiert und bewertet auch den Systemzustand des überwachten Systems und der Objekte auf dem überwachten Computer und meldet ihn an den Managementserver zurück. Ändert sich der Systemzustand eines überwachten Objekts oder werden andere Kriterien erfüllt, kann der Agent eine Warnung auslösen. Auf diese Weise wird das Bedienpersonal darüber informiert, dass etwas beachtet werden muss. Durch die Bereitstellung von Zustandsdaten über das überwachte Objekt an den Managementserver, liefert der Agent eine aktuelle Übersicht über den Zustand des Systems und aller Anwendungen, die es hostet(Microsoft, 2021).

Kommunikation zwischen Server und Agenten

Der Operations Manager Agent übermittelt Alarm- und Erkennungsdaten an den primären Managementserver, der diese wiederum in die Betriebsdatenbank schreibt. Der Agent sendet

außerdem Ereignis-, Leistungs- und Zustandsdaten an den primären Managementserver, welcher die Daten gleichzeitig in die Betriebs- und Data-Warehouse-Datenbank schreibt.

Der Agent sendet Daten gemäß den Parametern in regelmäßigen Abständen für jede Regel und jeden Überwachungsmonitor. Bei optimierten Erfassungsregeln werden Daten nur dann übertragen, wenn eine Abweichung eines Zählers von der vorherigen Stichprobe um eine bestimmte Toleranz vorliegt. Dies trägt dazu bei den Netzwerkverkehr und die in der Datenbank gespeicherte Menge an Daten zu reduzieren.

Darüber hinaus senden alle Agenten in regelmäßigen Abständen ein Datenpaket, den so genannten Heartbeat, an den Managementserver. Der Zweck des Heartbeats ist die Überprüfung der Verfügbarkeit des Agenten und der Kommunikation zwischen dem Agenten und dem Managementserver (siehe Abbildung 15)(Microsoft, 2021).

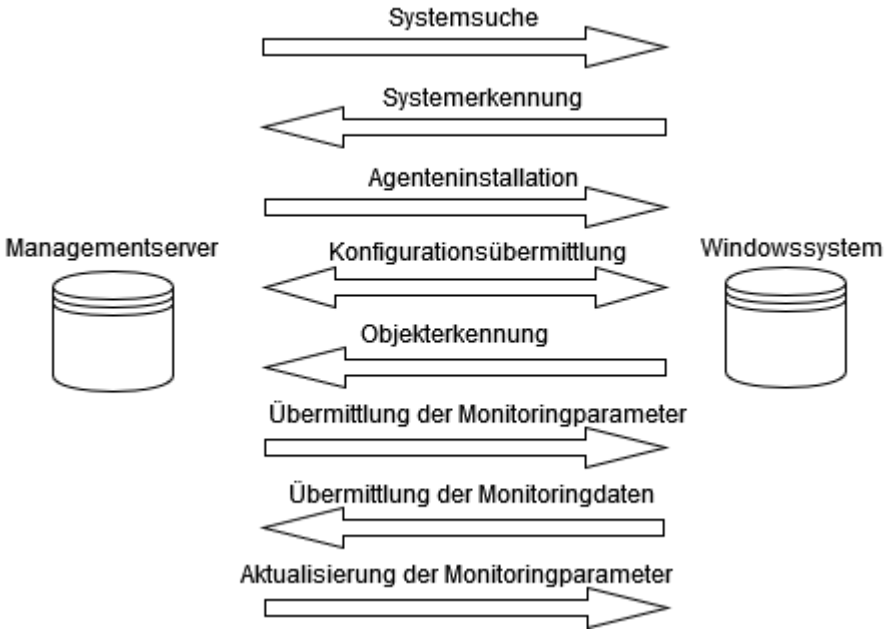

Abbildung 15: Prozess der Objekterkennung und Objektmonitoring in SCOM (in Anlehnung an Microsoft, 2021)

4 SITUATIONSANALYSE PANDEMIE

Im Kapitel der Situationsanalyse der Pandemie wird auf die sich geänderte Situation eingegangen und Informationen zur Krankheit selbst erörtert. Es werden die Auswirkungen auf Organisationen, Maßnahmen zur Weiterführung des Betriebs und Auswirkungen für IT-Organisation beziehungsweise der IT-Servicebereitstellung und Servicequalität eingegangen. Zudem wird dargelegt welche Kennzahlen und Schritte helfen können den Betrieb der IT-Infrastruktur und das Monitoringsystemen zu erleichtern.

4.1 Auswirkung auf Organisationen

Effekte von Gefährdungen wie es eine Pandemie ist, können laut Spörrer in nachfolgend aufgeführten Kategorien aufgeschlüsselt werden: (Spörrer, 2014)

- Engpass in der Liquidität
- Umsatzeinbruch
    - Gesetzliche Einschränkungen in der Abwicklung von Kundenkontakt
    - Änderungen der Auftragslage durch weniger Nachfrage oder Lieferproblemen
- Verhinderung von Anwesenheit der Angestellten (siehe nachfolgende Punkte)
- Gesetzliche Einschränkung der Organisation aufgrund von Schließungen

Ergänzend hierzu werden von Gregory für den Fall einer Gefährdung, in diesem Fall eine Pandemie, weitere Effekte und Auswirkungen kategorisiert: (Gregory, 2008)

- Unerreichbarkeit
    - Gesetzliche Änderungen in der Belegung oder dem Zugang zu öffentlichen und privaten Räumlichkeiten
- Ausfall von Versorgungsinfrastruktur
    - Lieferkettenunterbrechungen
    - Energieversorgung
- Unterbrechungen von Transportationsmöglichkeiten
    - Personal für öffentliche Transportmittel kann genauso von Einschränkungen oder Auswirkungen betroffen sein und sich daher auf die Verfügbarkeit negativ auswirken.
- Unterbrechung der Kommunikationswege
    - Kommunikationswege können in Spezialfällen die Auswirkungen einer Überbuchung beziehungsweise Überbeanspruchung der Technologien besonders

in Mitleidenschaft gezogen werden und zwischenzeitlich für Unzuverlässigkeit in der Kommunikationsabwicklung sorgen.

- Ortsbeschränkungen
    - Katastrophenereignisse können den Zutritt und das Verlassen von Orten einschränken (Ausreisebeschränkung).
- Abwesenheit von Arbeitskräften (Bundesamt für Sicherheit in der Informationstechnik, 2020)
    - Infektion und dadurch Absonderung
    - Vorsorgliche Absonderung aufgrund eines Verdachtsfalls (Kontaktpersonen von nachweislich positiv getesteten Personen)
    - Ausweitung des familiären Pflegebedarfs aufgrund von partiellen Überlastungen des Gesundheitssystems
    - Verfügbarkeit von Betreuungseinrichtungen durch Personal- und Kapazitätseinschränkungen
    - Allgemeine Vermeidung von Kontakten mit außerfamiliären Personen wie in öffentlichen Verkehrsmitteln

4.1.1 Verbreitungswege von COVID-19

Im Kontext der Auswirkungen der Coronavirus-Krankheit-2019 (COVID-19) auf Organisationen, wird in diesem Abschnitt erörtert, wie sich diese Krankheit verbreitet und welche Auswirkungen sich dadurch auf zwischenmenschlichen Kontakten ergeben. Mit aktuellem Wissensstand wird davon ausgegangen, dass das hauptsächliche Infektionsgeschehen zwischen Menschen stattfindet. Es kann jedoch nicht ausgeschlossen werden, dass asymptomatische Personen das Virus auch verbreiten, was gezielte Maßnahmen zur Unterbrechung von Infektionsketten zusätzlich erschwert (National Center for Immunization and Respiratory Diseases, 2020).

COVID-19 verbreitet sich, wenn eine infizierte Person Flüssigkeitströpfchen und sehr kleine Partikel ausatmet, die das Virus enthalten. Diese Tröpfchen und Partikel können von anderen Personen eingeatmet werden oder auf deren Augen, Nasen oder Mund gelangen. Unter Umständen können sie auch Oberflächen kontaminieren, mit denen die infizierte Person in Berührung gekommen ist. Menschen, die sich näher als einen Meter von der infizierten Person entfernt aufhalten, sind am ehesten gefährdet, sich anzustecken (National Center for Immunization and Respiratory Diseases, 2020).

4.2 Maßnahmen zur Weiterführung des Betriebs

In diesem Abschnitt werden Maßnahmen vorgestellt, welche die Durchführung von Geschäftsprozessen, unter Einhaltung von gesetzlichen Rahmenbedingungen der COVID-19 Pandemie, unterstützen.

4.2.1 Telearbeitsplatz und Fernzugriff

Vorausgesetzt die Arbeitsprozesse sind nicht an den Firmenstandort gebunden, können Angestellte mittels technischer oder organisatorischer Maßnahmen auch von Zuhause (Teleworking) diese Arbeiten durchführen. Diese Form der Arbeit erweist sich als äußerst praktikabel in Kombination mit räumlichen Einschränkungen der Zusammenarbeit, da der Arbeitsort von Angestellten flexibel auf laufende Anforderungen adaptiert werden kann (Bundesamt für Sicherheit in der Informationstechnik, 2008).

Im Zuge der Umsetzung gibt es auch zu bedenken, wie Arbeitsgeräte, (Sicherheits-) Updates und verschlüsselte Fernzugriffe auf interne Daten und Services abgehandelt werden müssen, um keine Abstriche in Punkto Datensicherheit eingehen zu müssen.

Hierbei eignet es sich aus technischer Sicht jedenfalls ein Monitoring und/oder ein Mobile-Device-Management (MDM) System zu implementieren. Dadurch wird proaktiv auf Risiken aufmerksam gemacht und gleichzeitig werden Personalressourcen in Bezug auf manuelle Wartungs- und Unterstützungstätigkeiten verringert.

MDM Systeme helfen, eine zentralisierte Umgebung für die Verwaltung und Wartung von Clientendgeräten bereitzustellen. Eine übliche Architektur der Implementierung ist eine Client-Server Kommunikation. Diese basiert auf Softwareagents (Endclient Software Installationen), welche den Server in vorgegebenen Intervallen kontaktieren und über den Zustand der zuvor definierten Kennzahlen informieren. Je nach Definition und Ausprägung der Informationstiefe, können diese Kennzahlen den Betrieb von folgenden Teilbereichen der IT-Infrastruktur erleichtern: (Kersten & Klett, 2017)

- Endgerätinventarisierung
- Zentrale Verwaltung und Ausrollung von Richtlinien (Gruppenrichtlinien)
- Zentralisierte Softwareverteilung (mittels Softwarepaketen) und für den Endbenutzer unsichtbare Installationen
- Freigabe und Installation von getesteten und verifizierten (Sicherheits-)Updates für Software und Betriebssysteme
- Ableitung von Problemen anhand von technischen Kennzahlen (wie beispielsweise folgende:)
    - CPU-Auslastung
    - Netzwerkbandbreite
    - Kritische Systemevents

    - Sicherheitsrelevante Ereignisse
- Abwicklung sicherheitsrelevanter Aufgaben wie Sperrung und Löschung eines Endgeräts bei Verlust oder Diebstahl
- Umsetzung einer einheitlichen Strategie zur Abhandlung von Backups und Wiederherstellungspunkten

4.3 Auswirkungen auf IT

Die in Abschnitt 4.2 erwähnten Maßnahmen können sich auf Themen in Punkto Sicherheit und IT-Operations beim Einsatz von Teleworking Arbeitsplätzen auswirken. Aufgrund der Implementierung von Arbeitsplätzen außerhalb des ständigen Arbeitsortes kann ein Unternehmen mit Problemen aus folgenden Themenbereichen konfrontiert werden (Kersten & Klett, 2017):

Verlust oder Diebstahl von Clientendgeräten

Bedingt durch den Wechsel der Arbeitsumgebungen steigt das Risiko eines Verlusts sowie Diebstahls gegenüber einem stationären Arbeitsgerät am ständigen Arbeitsort. Aus diesem Grund ist es empfohlen, die Möglichkeit einer schnellen Reaktion im Falle der oben erwähnten Spezialfälle gewährleisten zu können, bevor diese eintreten und somit auch die Informationssicherheit von Organisationsdaten vor Fremdzugriff schützen zu können. Dies kann mit Maßnahmen aus der Ferne über eine Verwaltungssoftware (MDM) geschehen und sich in Löschung und Sperrung ausdrücken.

Bring-Your-Own-Device und Sicherheitsrichtlinien

Aufgrund der heterogenen Eigenschaften von Endgeräten der Mitarbeiter*innen, welche für die Arbeitsabwicklung genutzt werden (BYOD), können zentralisierte Sicherheitsrichtlinien (meist über eine zentrale Instanz eines Domänencontrollers) nicht oder nur bedingt angewendet werden. Es wird empfohlen diese Randfälle mittels anderer Zugriffsmöglichkeiten (Sandbox, Webclient, Jumphost) abzuwickeln, da hier das Sicherheitsrisiko ausgehend von einem schadhaften Endgerät minimiert werden kann. Ein Sicherheitsrisiko kann auf mobilen Endgeräten (Smartphone, Tablet) aufgrund von Umgehung der Sicherheitsmerkmale sowie Sicherheitsrelevante Update oder unvorsichtiger Umgang entstehen.

Unzuverlässiger Internetzugang

Einschränkungen in der Reliabilität (Verbindungsabbrüche, Überlastung des Mobilfunknetzes, Überbuchung von Internetleitung) bei der Durchführung von Arbeitsprozessen aufgrund von instabiler Fernzugriffen über das Internet können den Einsatz von Teleworking Arbeitsplätzen enorm einschränken. Daher ist eine Gewährleistung eines zuverlässigen, nicht öffentlichen Internetzugangs, für die Integrität der Übertragung essentiell.

Compliance der Organisationsrichtlinien

Zentral verwaltete, ausgerollte und zugängliche Richtlinien in der Geräteverwaltung sind für die Zuverlässigkeit einer verlässlichen Anwendung von Sicherheitsstandards von großer Wichtigkeit. Dies kann nur gewährleistet werden, wenn die Endgeräte in Teleworking Arbeitsplätzen auch in regelmäßigen Abständen mit dem Organisationsnetzwerk verbunden werden (etwa über VPNs). Ansonsten können sich inkonsistente Zustände der Gerätecompliance entwickeln und zu weiteren, gröberen Problemen führen.

5 HYPOTHESENBILDUNG

Das Kapitel der Hypothesenbildung handelt von der Bildung und Herleitung der Hypothesen, welche im Rahmen dieser Arbeit untersucht werden. Es werden auch allgemeine Kriterien angeführt, welche von wissenschaftlichen Hypothesen erfüllt werden müssen.

Aufbauend auf die erörternde Themengebiete von IT-Service Management, Monitoring und den Kontext der Pandemie von COVID-19, wurden Hypothesen abgeleitet, wie sich die Anforderungen aufgrund des vermehrten Einsatzes von Teleworking Arbeitsplätzen in der Situation Pandemie an Monitoring Kennzahlen verändert haben.

Auf Basis der Literaturanalyse entwickelten Hypothesen wird mithilfe einer empirischen Untersuchung die Forschungsfrage dieser Arbeit untersucht (Raithel, 2008). Aufgrund der Unterscheidung zwischen allgemeinen Aussagen, welche sich von wissenschaftlichen Aussagen und daran gemessene Kriterien unterscheiden, müssen folgende Unterscheidungspunkte erfüllt werden (Bortz & Döring, 2006, S. 5):

1. „Eine wissenschaftliche Hypothese bezieht sich auf reale Sachverhalte, die empirisch untersuchbar sind.
2. Eine wissenschaftliche Hypothese ist eine allgemein gültige, über den Einzelfall oder ein singuläres Ereignis hinausgehende Behauptung (»All-Satz«).
3. Einer wissenschaftlichen Hypothese muss zumindest implizit die Formalstruktur eines sinnvollen Konditionalsatzes (»Wenn-dann-Satz« bzw. »Je-desto-Satz«) zugrunde liegen.
4. Der Konditionalsatz muss potenziell falsifizierbar sein, das heißt, es müssen Ereignisse denkbar sein, die dem Konditionalsatz widersprechen.“

5.1 Hypothese 1

Beginnend mit der ersten Hypothese der empirischen Untersuchung wird der Aspekt des Monitorings zur im Rahmen von ITSM beschriebenen Performance betrachtet. Im Kontext der Serviceerbringung der IT soll der Zusammenhang zu vermehrtem Einsatze von Teleworking Arbeitsplätzen und die Auswirkungen auf eben erwähnte Performance der Services untersucht werden.

Daraus ergibt sich die Hypothese 1: „Vermehrter Einsatz von Teleworking Arbeitsplätzen im Rahmen der Pandemie von COVID-19 hat die Anforderungen an IT-Services im Bezug von technischen Leistungsmerkmalen in der Serviceerbringung verändert.“

5.2 Hypothese 2

In Kapitel 2 wird auf ITSM eingegangen mit besonderem Fokus auf Abschnitt 2.6.3 mit einer beispielhaften Prozessbeschreibung sowie den Abschnitten 2.6.4 und 2.6.5 für die kundenorientierten Sichtweise und Zusicherung der vereinbarten Servicequalität. Hierbei lässt sich ableiten, dass sich Änderungen an den Anforderungen der Serviceerbringung auch Anpassungen dieser erfordern. Diese Anpassungen und Auswirkungen können mithilfe des Einsatzes einer Monitoringlösung validiert werden.

Folglich lautet die Hypothese 2: „Aufgrund von Anpassungen an der Serviceerbringung konnten, die sich geänderten Anforderungen an IT-Services für Teleworking Arbeitsplätze die geforderte Servicequalität ohne merkbare Einschränkungen beibehalten."

5.3 Hypothese 3

Wie in den Abschnitten 2.6 und 2.8 näher beschrieben, ist ein essentieller Teil der Servicebereitstellung von CSI. Mithilfe dieses Tools kann für Servicebezieher ein Mehrwert in der Qualität der Serviceerbringung geschaffen und zukünftig stetig und zielorientiert auf etwaige Änderungen der Rahmenbedingungen eingegangen werden.

Hierdurch wird die Hypothese 3 wie folgt abgeleitet:

„Durch erhöhten Fokus auf den Einsatz und Adaption von Monitoringlösungen kann die Servicequalität kontinuierlich verbessert werden"

6 METHODISCHE VORGEHEN

In diesem Kapitel und den zugehörigen Abschnitten wird das Untersuchungsdesign beschrieben. Anfangs wird mit der allgemeinen Beschreibung von empirischen Untersuchungsmethoden begonnen, gefolgt mit den herangezogenen Untersuchungsgruppen von Experten, anschließend wird die empirische Vorgehensweise der Experteninterviews erläutert. Nachfolgend wird auf den Interviewleitfaden und dessen Aufbau eingegangen. Dieser widmet sich der Erklärungsphase mittels Einleitungsfragen zu den zuvor festgelegten Hypothesen, Fragen zu den Hypothesen selbst und abschließenden Fragen.

6.1 Qualitative Forschung

Die Rahmenbedingungen der qualitativen Untersuchung widmen sich folgenden Punkten, um allen befragten Personen als Interviewer genügend Informationen sowie ein professionelles Interviewkonzept für das Ziel der Untersuchung darlegen zu können: (Raithel, 2008)

- Darlegung des Untersuchungsgegenstandes selbst
- Erklärung des Fragebogens und darin enthaltener Fragen, besonderer Eigenschaften der Fragestellung
- Details zur Einführung
- Kontaktaufnahme der ausgewählten Personen
- Neutrale Herangehensweise

6.2 Quantitative Forschung

Die quantitative Forschung wurde auf Basis der gewählten Forschungsfrage nicht als Untersuchungsinstrument gewählt, hat jedoch in ausgewählten Situationen, beispielsweise als schriftliche Befragung (im Setting einer internetgestützten Befragung), besondere Eigenschaften und Vorteile gegenüber einer qualitativen Forschungsmethode mit mündlichen Experteninterviews.

Diese Vorteile bei der Umsetzung lassen sich wie folgt beschreiben: (Raithel, 2008)

- Geringerer Ressourcenbedarf (Zeit- und Personalersparnis)
- Zeitliche Flexibilität bei der Beantwortung (und dadurch auch mehr Zeit, um über Frage nachzudenken)
- Standardisierung der Antwortformen und Antwortmöglichkeiten

Diesen Vorzügen stehen jedoch gleichermaßen Nachteile in folgenden Ausprägungen gegenüber: (Raithel, 2008)

- Keine Kontrolle über die Befragungssituation
- Verständnisprobleme bei Fragestellungen
    - Keine Möglichkeit zur Hilfe bei Verständnisproblemen
- Antwortgüte (unvollständige oder keine Antwort)

6.3 Beschreibung der Experten

Um die gewählten Hypothesen im Rahmen dieser Arbeit bearbeiten zu können, ist es essentiell die richtigen Experten auszuwählen um genügend Einblicke in deren Erfahrungswerte sowie daraus abgeleitete Informationen zu erhalten. Es stellt sich die Frage, welche Personenkreise Experten sind und welche Eigenschaften diese besonders auszeichnet. Einleitend kann gesagt werden, dass Experten über besonderes fachspezifisches Wissen verfügen. Die durchführende Person der empirischen Erhebung, in diesem Fall der Interviewer, muss entscheiden, welche Personen über adäquate Kenntnisse verfügen um die Interviewfragen inhaltlich ausreichend beantworten zu können. Weiters ist entscheidend, abzuschätzen welche Personen willig und fähig sind, ihr Fachwissen in geeigneter Form weitergeben zu können (Gläser & Laudel, 2009).

Auf Basis der angeführten Informationen, aus der Literatur, ist die Untersuchungsgruppe dieser Erhebung ein Personenkreis, welcher in einer IT-Administrations- sowie IT-Beratungsfunktion mit mindestens einer Lösung aus dem Bereich Monitoring gearbeitet (Implementierung, Betreuung oder Administration) hat.

Im Rahmen der Erhebung wird mit vier Experten jeweils ein Interview geführt. Um ein möglichst breites Fachwissen der Experten abfragen zu können, wird besonders auf Praxiserfahrung im zuvor definierten Bereich, in mehr als einer Infrastrukturumgebung, Wert gelegt. Dies kann optimalerweise erreicht werden, wenn Experten bei einem Dienstleister für IT-Infrastruktur beschäftigt sind oder waren, wo Wissen und Erfahrung aus vielen Unterschiedlichen Kundenprojekten und -typen gesammelt werden, kann oder konnte.

Es wurden drei IT-Consultants für Infrastrukturthemen und eine Person aus der IT-Operations Abteilung ausgewählt und befragt. Die Eigenschaften dieser befragten Personen lassen sich in folgenden Punkten beschreiben:

- Alle Experten haben Erfahrung mit mindestens einer Monitoringlösung.
- Alle Experten haben mehr als vier Jahre Erfahrung im Bereich IT-Infrastruktur Betreuung, Administration oder Projektmitarbeit.
- Alle Experten haben bei mindestens einer Unternehmensinfrastruktur mitgewirkt.
- Sie haben Erfahrung mit Monitoringlösungen bei mindestens einer Infrastrukturumgebungen gesammelt.

- Im geplanten Durchführungszeitraum, November 2021, haben die Experten zeitliche Ressourcen für ein virtuelles Interview über Microsoft Teams.
- Sie sind mit der Aufzeichnung und anonymen Aufbereitung in dieser Arbeit einverstanden.
- Bereit ihre Erfahrungen und angeeignetes Wissen im Rahmen der Befragung zu teilen.

6.4 Experteninterviews

Im Untersuchungsdesign dieser empirischen Forschung wurden Experteninterviews mit Einzelpersonen durchgeführt. Der Aufbau des in Abschnitt 6.6 beschriebenen Gesprächsleitfadens gibt den Experteninterviews einen teilstrukturierten und teilstandardisierten Charakter (Raithel, 2008). Die Durchführung wird aufgrund der geographischen Distanz und der Situation einer Pandemie ausschließlich digital über Videokonferenzen durchgeführt.

Aufgrund der gewählten Durchführungsform lässt sich weniger Einfluss auf die Gesprächssituation und Qualität der Erhebung ausüben. Einfluss auf die Qualität könnten unter anderem ein störungsfreier Raum zur Durchführung sein, oder in der Form eines Face-to-Face Interviews was die Einschränkung Nebentätigkeiten verhindert. Zusätzlich kann mithilfe von Videokonferenzen näher auf die Körpersprache der befragten Personen, zum Inhalt der gestellten Fragen, eingegangen werden, was bei gewöhnlichen Telefonkonferenzen nicht möglich ist. Ebenso ist der Austausch von Unterlagen, besonders von Seiten der Experten ist im Rahmen von Videokonferenzen mittels Chatfunktion problemlos möglich, um erweiterte Informationen zu den hervorgehobenen Themenblöcken erhalten zu können (Gläser & Laudel, 2009).

6.5 Kontaktaufnahme

Um umfangreiche Information aus den Interviews generieren zu können, ist die Kontaktaufnahme und der Aufbau einer Beziehung wichtig. Im Rahmen der Kontaktaufnahme soll der Interviewpartner überzeugt werden an der Untersuchung teilzunehmen, sowie ein Vertrauen zum Interviewer aufgebaut werden. Die befragte Person soll zudem erfahren, wieso sie an der Untersuchung mitwirken und Zeit dafür investieren soll. Vorteilhaft ist es auch, eine schriftliche Ankündigung, Terminvereinbarung und den tatsächlichen Termin des Interviews selbst in kurzen zeitlichen Abständen abzuhalten, um die Anliegen beim Interviewpartner im Gedächtnis zu behalten (Gläser & Laudel, 2009).

6.6 Aufbau des Gesprächsleitfadens

In diesem Abschnitt wird der Aufbau und die Struktur des Gesprächsleitfadens näher beleuchtet. Dies dient zur weiteren Auswertung der Interviews, um ein möglichst standardisiertes und wissenschaftlich verwertbares Ergebnis ableiten zu können. Der Vorteil einer teilstandardisierten Vorgehensweise ist die Möglichkeit dem Interviewpartner offene Antwortmöglichkeiten zu bieten (Gläser & Laudel, 2009).

Wichtige Eckpunkte in der Gestaltung eines Interviewleitfadens sind folgende: (Gläser & Laudel, 2009)

- Fragen in leicht verständlicher Alltagssprache
- Meinungsfragen sind nur in Sonderfällen sinnvoll (wie Bewertungen oder Beweggründe)
- Simulationsfragen sind als Erzählanregung vorteilhaft
- Fragen nach Fakten sollen zur Anregung einer Erzählung dienen
- Anregungen zur genaueren Erzählung sind wichtiger als Detailfragen, da diese oft Details im Laufe der Erzählung mit sich bringen
- Klarheit der Fragestellung
- Provozierende Fragestellungen sind zur Anregung des Gesprächs nützlich, sollten jedoch sparsam eingesetzt werden
- Gewährleistung der Anonymität bei Fragestellung

Der Aufbau dieses Gesprächsleitfadens wird wie folgt gegliedert:

- Erklärungsphase
- Einleitungsphase
- Hauptphase
- Zusammenfassung

6.6.1 Erklärungsphase

Begonnen wird das Interview mit der Einführung des Gesprächspartners an die Interviewsituation, Ablauf und essentielle Informationen des Gesprächsthemas selbst. Zudem wird den befragten Personen der Gegenstand der Untersuchung dargelegt, um eine transparente und vertrauensvolle Gesprächsatmosphäre herzustellen. Weiters wird den Befragten mitgeteilt, dass die Teilnahme als Experte in dieser Untersuchung vertraulich behandelt wird, um eine offene Gesprächskultur zu fördern (Gläser & Laudel, 2009).

Den Befragten wurde erklärt, dass es das Ziel dieser Arbeit ist, wie sich mit vermehrtem Einsatze von Teleworking Arbeitsplätzen in der Pandemie von COVID-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert haben. Diese Zielformulierung wird den Experten am Ende der Befragung mithilfe der Aufgestellten Hypothesen nähergebracht, mit dem Augenmerk darauf sie nicht bereits im Vorhinein damit ungewollt zu beeinflussen.

Für effizientes und schnelles durchführen der Befragung und um zielgerichtete Antworten zu gewährleisten wurde der Kontext und Thematik von ITSM sowie Monitoring besprochen falls sich Fragen seitens der Experten ergeben haben.

6.6.2 Einleitungsfragen

Die Gespräche wurden mit allgemeinen Fragestellungen eingeleitet, um eine aufgelockerte Situation herzustellen. Ziel war es auch, mithilfe dieser leicht zu beantwortenden Fragen, zu eruieren, welche Vorerfahrungen der Experte zur befragten Thematik hat.

- Wie viele Jahre haben Sie bereits Erfahrung mit Monitoringlösungen für IT-Infrastruktur sammeln können?
- Wie viele Jahre haben Sie bereits Erfahrung in Betreuung, Administration oder Projektmitarbeit von IT-Infrastruktur sammeln können?
- Bei wie vielen Kunden waren Sie in der Administration, Betreuung oder Projektmitarbeit von IT-Infrastruktur beteiligt?
- Mit welchen Monitoringlösungen konnten Sie bereits Erfahrungen sammeln?

Darauffolgend wurde erklärt, wie der Hauptteil der Befragung durchgeführt wird.

6.6.3 Hypothese 1

„Vermehrter Einsatz von Teleworking Arbeitsplätzen im Rahmen der Pandemie von COVID-19 hat die Anforderungen an IT-Services im Bezug von technischen Leistungsmerkmalen in der Serviceerbringung verändert."

Wie zuvor in Abschnitt 5.1 dargelegt, ist das Ziel dieser Hypothese herauszufinden, wie sich der vermehrte Einsatz von Teleworking Arbeitsplätzen im Rahmen der Pandemie von COVID-19 die Anforderungen an IT-Services im Bezug von technischen Leistungsmerkmalen in der Serviceerbringung verändert hat.

1. Hat sich im Rahmen der Pandemie von COVID-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?
2. Wie haben sich, aufgrund des vermehrten Einsatzes von Teleworking, Anforderungen an die IT-Infrastruktur geändert?
3. Wie haben sich diese Änderungen der Anforderungen an die Infrastruktur ausgewirkt?

6.6.4 Hypothese 2

„Aufgrund von Anpassungen an der Serviceerbringung konnten, die sich geänderten Anforderungen an IT-Services für Teleworking Arbeitsplätze die geforderte Servicequalität ohne merkbare Einschränkungen beibehalten."

Im nächsten Schritt wurde, wie schon in Abschnitt 5.2 erklärt, die Hypothese 2 behandelt. Ziel hierbei war es herauszufinden, ob aufgrund von Anpassungen an der Serviceerbringung, die geforderte Servicequalität ohne merkbare Einschränkungen beibehalten werden konnte.

1. Hat der vermehrte Einsatz von Teleworking Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Serviceumgebungen?
2. Falls ja, wie haben sich diese Auswirkungen bemerkbar gemacht?
3. Mussten Aufgrund dieser wandelnden Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Servicequalität beibehalten zu können?
4. Wenn ja, welche Maßnahmen wurden gesetzt?
5. Haben diese Maßnahmen die Servicequalität in zufriedenstellenden Maß verbessert?

6.6.5 Hypothese 3

„Durch erhöhten Fokus auf den Einsatz und Adaption von Monitoringlösungen kann die Servicequalität kontinuierlich verbessert werden"

Ausgehend von der Hypothese 3, welche in Abschnitt 5.3 dargelegt wird, wurde bei den Experten abgefragt, inwieweit ein erhöhter Fokus auf den Einsatz und der Adaption von Monitoringlösungen hilft, die die Servicequalität kontinuierlich verbessern zu können.

1. Inwiefern helfen Monitoringlösungen den laufenden Betrieb von IT-Services und Infrastruktur zu unterstützen?
2. Gibt es Fälle, in denen der Einsatz von Monitoringlösungen keinen Mehrwert bringt?
    a. Welchen Grund hat dies?

6.6.6 Abschließende Fragen

Am Ende jeder individuellen Befragung war es wichtig die Meinung der befragten Personen sowie ein Feedback zu den gestellten Fragen zu erhalten. Abschließend wurde sich für die Mitwirkung an der Befragung bedankt. Zudem wurde dem Gesprächspartner mitgeteilt, dass nun die Befragung abgeschlossen ist. Die Möglichkeit zur Beantwortung noch offener Fragen Gesprächspunkte von Seiten der befragten Person wurde eingeräumt. Mithilfe dieses Vorgehens kann sichergestellt werden, den Befragten abholen zu können und vollumfänglich zu Wort kommen zu lassen (Gläser & Laudel, 2009).

1. Wie haben Sie das Interview empfunden?
2. Haben Sie noch Anmerkungen zu den Fragen?
3. Haben Sie noch zusätzlichen Input zum Forschungsthema?

6.7 Tools

Wie bereits in Abschnitt 6.3 erwähnt, wurde für die Abhaltung der Interviews Microsoft Teams mit der integrierten Aufzeichnungsfunktion verwendet. Für die Transkription wurde rev.ai [1]verwendet und im Rahmen der Paraphrasierung mit MAXQDA auf etwaige Fehler untersucht und verbessert. Die Codierung der Paraphrasen wurde mit demselben Tool, MAXQDA, umgesetzt.

6.8 Durchführungszeitraum

Die Interviews der vier Experten wurden von 05.11.2021 bis 19.11.2021 durchgeführt. In diesem Zeitraum fand die Kontaktaufnahme via Mail und Microsoft Teams, Vorgespräch zur Thematik des Gesprächs sowie das Interview selbst statt.

Die Audiodateien und Transkripte der geführten Gespräche sind der beigelegten CD zu entnehmen.

6.9 Dokumentationsform

Für die Gewährleistung der Balance zwischen Praktikabilität, Umfang und tiefe der Dokumentationsqualität, gilt es folgende Punkte zu beachten: (Bogner et al., 2014)

- Unter- und Überdokumentation von Informationen vermeiden
- Informationsverlust bei Verzicht von Audioaufzeichnungen
    - Falls kein gleichwertiger Gesprächsersatz gefunden werden kann, handschriftliche Gesprächsnotizen möglich
    - Gesprächsnotizen müssen nicht wörtlich jedes Wort des Gesprochenen beinhalten, was auch in der Natur eines Gesprächs nicht möglich wäre, sondern es ist ausreichen eine thematische oder inhaltliche Zusammenfassung des gesagten zu liefern
- Qualität der Aufzeichnung, falls Zustimmung der befragten Personen zu einer grundsätzlichen Aufzeichnung gegeben ist

[1] https://www.rev.ai/

- Vermeidung von Videoaufzeichnungen, da dies die Situation des Interviews belasten kann

Zudem wird auch erwähnt, besondere Eckpunkte für die Erarbeitung der Transkription zu beachten: (Bogner et al., 2014)

- Vollständige Transkription der Aufnahmen
- Aufteilung in Fragen und den dazugehörigen Antworten
- Inhalt der gesprochenen Sprache sinngemäß mit richtiger Grammatik in üblicher Schriftsprache adaptieren
- Dokumentation von auffälligen Situationen, wie etwa längere Pausen oder nonverbale Kommunikation wie lachen

6.10 Qualitative Inhaltsanalyse nach Mayring

In diesem Abschnitt wird, die von Mayring bewährte Methode zur strukturierten Auswertung für Daten beschrieben. Auf Basis der transkribierten Interviews werden Methoden zur Analyse mithilfe von Kategorienbildung durchgeführt. Das Ziel der qualitativen Inhaltsanalyse nach Mayring ist es Kommunikationen nach folgenden Eigenschaften zu analysieren: (Mayring, 2015)

- Systematisch
- Regelgeleitet
- Theoriegeleitet

Diese dienen als Hilfestellung um Rückschlüsse auf Teilaspekte der Untersuchungsform zu identifizieren.

6.10.1 Grundprinzipien

Mit den Grundprinzipien nach Mayring werden essentielle Punkte angeführt und beschrieben, welche in der qualitativen Inhaltsanalyse Beachtung finden sollen: (Mayring, 2015)

- Das zu analysierende Textmaterial (in diesem Fall das transkribierte Experteninterview) soll im Kontext des Gesprächs interpretiert werden. Hierbei kann mittels Referenzen nach der Schlussfolgerung und Interpretation argumentiert werden, um eine transparente Verknüpfung darzulegen
- Wie bereits in Abschnitt 6.10 begonnen, soll eine Inhaltsanalyse mit den Grundprinzipien von Mayring systematisch und regelgeleitet sein. Es werden im Zuge der Inhaltsanalyse ein Regelwerk und Werkzeuge vorbereitet und angewandt. Dieses Vorgehen gewährleistet Nachvollziehbarkeit für Dritte für den wiederholten Einsatz dieses Vorgehens.

- Durch eine konsequente Definition und Anwendung von Kategorien wird die Zuordnung von Textbausteinen nachvollziehbar und transparent aufbereitet. Eine Vergleichsbasis für abgeleitete Ergebnisse wird geschaffen.
- Anwendung der Techniken auf den Untersuchungsgegenstand festlegen, und nicht rein technikgeleitet arbeiten. Hierbei wird die Orientierung am zu analysierenden Material in den Vordergrund gerückt und nicht der „one-fits-all“ Ansatz verwendet.
- Die Vorabprüfung mittels einer Pilotstudie ist essentiell, um zu identifizieren, ob die festgelegten Regelwerke und Werkzeuge sowie die Kategorisierung von Textbausteinen als ausreichend und zielgerichtet für die Auswertung sind.
- Der Einbezug von quantitativer Analyseschritte zur Begründung generalisierter Ergebnisse können sinnvoll sein und den Argumentationsstandpunkt sinnvoll darlegen.
- Reliabilität und Validität des Vorgehens sollen die Analyse während des gesamten Prozesses begleiten und nicht am Ende der Einschätzung einmalig angewendet werden. Hierbei wird die flexible Ausgestaltung methodischer Standards des Vorgehens mit objektiven Gütekriterien verknüpft.

6.10.2 Grundformen

Bei den Grundformen der qualitativen Inhaltsanalyse handelt es sich um die: (Mayring, 2015)

- Zusammenfassung
    - Diese zielt auf die Reduktion des verwendeten Materials ab, um schlussendlich nur noch das Forschungsthema wesentliche Passagen weiter zu verwenden. Diese Verdichtung der Inhalte soll jedoch die Repräsentation des ursprünglichen Textmaterials beibehalten.
- Explikation
    - Sie ergänzt das vorhandene Textmaterial mit erklärenden Bausteinen, um das Gesamtverständnis der Inhalte zu erweitern.
- Deduktion
    - Anwendung der zuvor gewählten Kategorien auf die zusammengefassten Textbausteine
- Strukturierung
    - Das Textmaterial wird mittels Instrumente, wie beispielsweise ein Kodierleitfaden, aufgeteilt, zugeordnet und ausgewertet.

6.10.3 Kategorienbildung

Die Kategorien, welche für die deduktiven Kategorienanwendungen und für die Zuordnung der Textpassagen verwendet werden, basieren auf die zuvor erstellten Hypothesen und stellen sich wie folgt zusammen:

Hypothese 1:

„Vermehrter Einsatz von Teleworking Arbeitsplätzen im Rahmen der Pandemie von COVID-19 hat die Anforderungen an IT-Services im Bezug von technischen Leistungsmerkmalen in der Serviceerbringung verändert."

→Kategorie: Änderung in IT-Serviceerbringung

Hypothese 2:

„Aufgrund von Anpassungen an der Serviceerbringung konnten, die sich geänderten Anforderungen an IT-Services für Teleworking Arbeitsplätze die geforderte Servicequalität ohne merkbare Einschränkungen beibehalten."

→Kategorie: Maßnahmen zur Einhaltung der IT-Servicequalität

Hypothese 3:

„Durch erhöhten Fokus auf den Einsatz und Adaption von Monitoringlösungen kann die Servicequalität kontinuierlich verbessert werden"

→Kategorie(n): Einsatz von Monitoring(lösungen), Monitoringkennzahlen

6.11 Paraphrasierung

Um die Paraphrasierung, mithilfe von MAXQDA, verdeutlichen zu können, wird auszugsweise ein Beispiel des transkribierten Gespräches mit einer Paraphrase in Tabelle 3 angeführt.

Transkript	Paraphrase
Anfangen tut es eigentlich bei Updates. Es ist schwieriger, die Clients in einer vernünftigen Zeit zu erwischen. Und zum Beispiel Installationen, die wichtig sind, rauszupushen etc., weil die Clients nicht immer online sind ja, diese ganze Push Mechanismus ist auf jeden Fall deutlich schwerer, was wiederum dazu führt, dass man Clients Zugriff gewährt, die nicht den Security Einstellungen entsprechen, die über normalerweise Active Directory oder so verteilt werden, sondern halt ja keine oder schlechte Einstellungen haben.	Clientverwaltung, Update Compliance, Software Compliance sind aufgrund der heterogenen Umgebungen schwerer geworden einzuhalten; Führt beim Zugriff in Firmennetzwerke zu Security Risiken

Tabelle 3: Darstellung Paraphrase

6.12 Kategorisierung

Die Kategorisierung wurde wie in Tabelle 4 beispielhaft entnommen, um das Vorgehen zu verdeutlichen.

Dokument	**Paraphrasen**	**Codes**	**Paraphrasiertes Segment**
Experteninterview4, Pos. 16	Ja negative Auswirkungen gerade im Aspekt der Clientverwaltung und Security	Auswirkungen auf Infrastruktur	Ähm, zumindest was den Aspekt Sicherheit betrifft, auf jeden Fall. Es gibt die Schwierigkeit, dass man Clients, die nicht im eigenen Haus stehen oder nicht im LAN stehen, sondern irgendwo im WAN sind, mit VPN verbunden sind, deutlich schwerer zu servicieren sind.
Experteninterview4, Pos. 16	Clientverwaltung, Update Compliance, Software	Auswirkungen auf Infrastruktur,	Anfangen tut es eigentlich bei Updates. Es ist schwieriger, die Clients in einer vernünftigen

	Compliance sind aufgrund der heterogenen Umgebungen schwerer geworden einzuhalten; Führt beim Zugriff in Firmennetzwerke zu Security Risiken	Monitoringkennzahlen	Zeit zu erwischen. Und zum Beispiel Installationen, die wichtig sind, rauszupushen etc., weil die Clients nicht immer online sind ja, diese ganze Push Mechanismus ist auf jeden Fall deutlich schwerer, was wiederum dazu führt, dass man Clients Zugriff gewährt, die nicht den Security Einstellungen entsprechen, die über normalerweise Active Directory oder so verteilt werden, sondern halt ja keine oder schlechte Einstellungen haben.
Experteninterview4, Pos. 20	Maßnahmen: VPN für Fernzugriff wenn möglich; Ansonsten Intensivierung des Einsatzes von Cloudmodellen	Änderung in IT-Serviceerbringung	Der einfachste Weg ist normalerweise immer eine VPN Verbindung, die stark genug ist und dies natürlich direkt abhängig von Internetleitung. Also zumindest da ist auf jeden Fall in den letzten Jahren einiges an Finanzen investiert worden. Und ja, wenn die Möglichkeit nicht gegeben ist, den Service on-premise oder in der eigenen Infrastruktur darzustellen, dann muss man auf einen Cloud Service gehen.

Tabelle 4: Darstellung Kategorisierung

Mit Fokus auf die Nachbereitung und Transkription der Gespräche, wurde bei noch unbekannten oder missverständlichen Formulierungen und Fachbegriffe nachgefragt, um eine klare Zuordnung zu ermöglichen.

7 ERGEBNISSE

Nachträglich kann die Zusammensetzung der Experten als sehr erfolgreich beschrieben werden, da unterschiedliche Blickwinkel und Erfahrungen zu einer sachlichen und professionellen Gesprächsbasis beigetragen haben.

Aufgrund der individuellen Projekt- und Kundenerfahrungen mit diversen und Grund auf verschiedenen Infrastrukturumgebungen konnte ein breites, aber auch tiefes Fundament an Erfahrung mithilfe der Fragen gewonnen werden konnte.

7.1 Einleitung

Beginnend mit den Einleitungsfragen, wird in Tabelle 5 zusammenfassend dargestellt wie sich die Erfahrung der befragten Experten zusammensetzt.

Paraphrasen
9 Jahre Erfahrung mit Monitoringlösungen
11 Jahre Berufserfahrung
Erfahrung bei drei Umgebungen plus Erfahrungsaustausch mit Kollegen
Erfahrung mit Nagios, WürthPhoenix NetEye, PRTG, Zabbix, upRobot, Splunk, Elasticsearch
mindestens 6 Jahre Erfahrung mit Monitoringlösungen
10 Jahre Erfahrung mit IT-Infrastruktur
Erfahrung bei 30-40 Kundensystemen
Erfahrung mit SCOM, Nagios, PRTG
22-23 Jahre Erfahrung mit Monitoring
über 20 Jahre Berufserfahrung
Erfahrung bei mehr als 100 IT-Systemen
15 Jahre Erfahrung mit Monitoringsystemen
15 Jahre Berufserfahrung
Erfahrung bei 10- 20 unterschiedlichen Umgebungen
Erfahrung beim Monitoring mit SCOM, PRTG, NAGIOS mit checkmk

Tabelle 5: Expertenzusammensetzung

Die Erfahrungseigenschaften der Experten können damit wie folgt zusammengefasst werden:

- Berufserfahrung
    - Diese lässt sich auf 10 bis über 20 Jahre zusammenfassen.
- Erfahrung mit Monitoringlösungen
    - Die Erfahrung mit Monitoringlösungen reicht von 6 bis 23 Jahre.
- Anzahl der Infrastrukturumgebungen
    - Die Erfahrung der Experten reicht von 3 bis zu mehr als 100 individuellen Kundensystemen. Dies lässt sich auf Basis ihrer Art der Tätigkeit, intern oder externe Rollen, begründen. Hier lässt sich ableiten, dass eine externe Rolle eines

IT-Consultants bei deutlich mehr Umgebungen Erfahrung sammeln konnte als eine interne Rolle einer Organisation.

- Monitoringlösungen
    - Die Experten konnten Erfahrungen mit den gängigen Monitoringlösungen Nagios, WürthPhoenix NetEye, PRTG, Zabbix, upRobot, Splunk, Elasticsearch, Microsoft System Center Operations Manager und checkmk sammeln.

7.2 Auswertung Hypothese 1

Mit Blick auf die Bestätigung von Hypothese 1, wurden Teilfragen gestellt und werden in diesem Abschnitt basierend auf den dazugehörigen Paraphrasen aus Tabelle 6 zusammengefasst.

„Vermehrter Einsatz von Teleworking Arbeitsplätzen im Rahmen der Pandemie von COVID-19 hat die Anforderungen an IT-Services im Bezug von technischen Leistungsmerkmalen in der Serviceerbringung verändert."

Paraphrasen
User haben erhöhte Servicequalität besserer Verfügbarkeit, mehr Flexibilität und Sicherheit, kaum Einschränkungen
Anforderungen haben sich bei Infrastruktur und Securitykonzepte verändert
Sofern es die Rolle erlaubt hat sich Teleworking merklich gesteigert
Teleworking merklich gesteigert seit Pandemie
Teleworking merklich gesteigert. Bestehende IT-Infrastruktur nicht ausreichend. Skalierbarkeit fraglich. Kapazitäten fraglich. Cloud Modelle eingesetzt. Kombination aus on-premise und Cloud erfordern angepasstes Monitoring
Wenn Infrastruktur skalierbar und Teleworking unterstützt wurde, weniger Probleme bei Umstellung. Sonst Umstellung aufwendig da Infrastruktur umgebaut oder erweitert werden muss
Seit Pandemie deutliche Steigerung von Teleworking Arbeitsplätzen bei Kundenumgebungen

Tabelle 6: Paraphrasen Hypothese - Frage 1 und 2

Somit kann auf Basis der paraphrasierten Expertenaussagen gesagt werde:

- Der Einsatz von Teleworking hat sich in der Pandemie von COVID-19 merklich gesteigert.
- Es haben sich durch diesen erhöhten Einsatz von Teleworking Arbeitsplätzen Änderungen an die Anforderungen von Sicherheitskonzepten, Skalierbarkeit, Einsatz von Cloudmodellen, Topologie beziehungsweise Architektur von IT-Infrastruktur ergeben.

7.3 Auswertung Hypothese 2

„Aufgrund von Anpassungen an der Serviceerbringung konnten, die sich geänderten Anforderungen an IT-Services für Teleworking Arbeitsplätze die geforderte Servicequalität ohne merkbare Einschränkungen beibehalten."

Anpassungen an die Serviceerbringung lassen sich in die Gebiete Maßnahmen für Infrastruktur, Sicherheitsmaßnahmen und organisatorische Maßnahmen gliedern. Die Zuordnung der Paraphrasen liegt den Tabellen Tabelle 7, Tabelle 8 und Tabelle 9 zugrunde.

- Maßnahmen für IT-Infrastruktur
    - Netzwerk und im speziellen VPN Zugriffe
    - Clients (standardisierte Hardware) und forciertes Clientmanagement
    - Monitoring wurde generell und speziell das Clientmonitoring erweitert
    - Implementierung von Cloud Modellen zur Serviceerbringung (statt ausschließlich on-premise Lösungen)
    - Auslagerung von IT-Ressourcen auf Cloud Modelle mit der Möglichkeit für Ressourcengruppen auf einen Pool an Rechenleistung zuzugreifen
- Sicherheitsmaßnahmen
    - Erweiterung oder Umplanung des Sicherheitskonzeptes
    - Änderung bei Netzwerktopologie und Segmentierung
    - Sicherheitskritische Praktiken wurden evaluiert und geändert
    - Multifaktor Authentifizierung
- Organisatorische Maßnahmen
    - Awareness Schulungen für Anwender und IT-Betrieb, um Sicherheit zu erhöhen
    - Regelung des Einsatzes von Teleworking standardisieren
    - Dokumentation der Benutzung erleichtert den Anwender*innen die Anwendung der Lösungen

Zusammenfassend lassen sich die Auswirkungen an die Servicequalität wie folgt gliedern:

- Positiv
    - Die Verfügbarkeit der Services wurde verbessert
    - Die Flexibilität in der Benutzung wurde erhöht
    - Die Sicherheit der Umgebungen von IT-Infrastruktur wurde erhöht
    - Bewusstsein der Wichtigkeit von IT-Infrastruktur wurde erhöht und dadurch Maßnahmen zur positiven Weiterentwicklung eingeleitet
    - Monitoringkonzept musste adaptiert werden um auf Clientmanagement und Sicherheitsthemen ausreichend reagieren zu können
    - Nutzung von Cloudmodellen für flexible Ressourceneinbindung und allgemeiner Skalierbarkeit

  - Sicherheitsvorteile in der Umstellung von Services welche statt on-premise über die Cloud angeboten wurden (Netzwerkkonfiguration, VPN)
  - Das Angebot an individuellen Cloudservices hat sich erhöht und dadurch die Serviceerbringung bei Inanspruchnahme auf individueller Basis erhöht.
- Negativ
  - Bei unzureichender Vorbereitung auf Teleworking kam es zu Einschränkungen in der Verfügbarkeit.
  - Anpassungen und dadurch erhöhter Ressourcenbedarf für Serviceerbringung nötig.
  - Wenn Bewusstsein für die Wichtigkeit von IT-Infrastruktur fehlte, war diese schlecht auf Teleworking und allen sicherheitsrelevanten Themen vorbereitet.
  - Komplexität bei Clientmanagement und Sicherheit wurde erhöht
  - Update und Software Compliance in heterogenen und dezentralen Umgebungen erschwert möglich und erhöht Risiken im Bezug auf den Zugriff non-compliant Clients
  - Aufkommen von Sicherheitsincidents hat sich bei Clients erhöht
  - Anforderungen an Netzwerkschnittstellen sowie die Zusammensetzung des Netzwerkverkehrs haben sich geändert und können problematisch für Serviceerbringung werden (mehr ingoing Traffic, wo zuvor hauptsächlich outgoing Traffic war und auch die Netzwerkschnittstelle dementsprechend dimensioniert war) sowie die
  - Einsatz von Cloudmodellen erfordert neues Wissen im Betrieb und erhöht Komplexität in der Fehlerbehebung aufgrund der zusätzlichen Zwischenebene
  - Auslagerung von Clientressourcen kann aufgrund von Latenzen die Servicequalität beeinträchtigen

Paraphrasen

User haben erhöhte Servicequalität besserer Verfügbarkeit, mehr Flexibilität und Sicherheit, kaum Einschränkungen
Anforderungen haben sich bei Infrastruktur und Securitykonzepte verändert
Es haben sich Anforderungen an Netzwerkinfrastruktur, Teleworkingclients, VPN Konfigurationen geändert
Anforderung an Anbindung gestiegen, weil Trafficaufkommen sich ändert
positive Auswirkungen auf Infrastruktur, weil Unternehmen Wichtigkeit der Infrastruktur wahrnehmen und Maßnahmen zur Absicherung einleiten.
Negative Auswirkungen bei schlechter Vorbereitung; Services können ausfallen, Verfügbarkeit eingeschränkt sein.
Security und Clientmanagement bei manchen Unternehmen und Folgen nicht bewusst; Geringes Bewusstsein und keine Maßnahmen zur Absicherung haben großes Sicherheitsrisiko
Trotz Teleworking bereits im Einsatz waren Optimierungen nötig.
Bewusstsein für IT-Infrastruktur als Rückgrat der Unternehmen fehlt noch; schlechte Absicherung führt zu Sicherheitsrisiken

Monitoringkonzept musste adaptiert und ausgebaut werden. Security und Clientmonitoring besonderer Stellenwert aufgrund der geänderten Anforderungen.
Altlasten wurden aufgrund der negativen Auswirkungen aufgerollt und nachgebessert. Kritische Infrastrukturthemen wurden angepasst, haben zu Verbesserungen geführt
Infrastruktur wurde vereinheitlicht im Zuge von Neuanschaffungen
Neue Infrastruktur musste in Monitoring eingebunden werden; wurde mit Vereinheitlichung vereinfacht.
Serviceerbringung hat sich geändert. User verteilt, heterogene Infrastruktur, neue Faktoren bei Servicequalität. Bestehende Services über Internet performant und Sicher. Führte zu Topologieänderungen; Auslagerung in Cloud
Cloud Services wurden implementiert. Bereitstellung über Cloud simpler als on-premise bei skalierbaren Services. Für Enduser kaum unterschied in Benutzung.
Auswirkungen: Je nach bestehender Ausrichtung; gar nicht oder sehr stark. Wenn Kunden bereits gut vorbereitet waren für Teleworking waren wenige Anpassungen nötig
Umsetzung als Cloud Applikation direkt und nicht nur auf Basis von IaaS mit eigener Lösung bei Kunden. Lösungen dieser Art bei bekannten Herstellern bereits in Angebot
Es wird sowohl bestehende Infrastruktur weiterbetrieben als auch Cloud Lösungen in Anspruch genommen.
Ja negative Auswirkungen gerade im Aspekt der Clientverwaltung und Security
Clientverwaltung, Update Compliance, Software Compliance sind aufgrund der heterogenen Umgebungen schwerer geworden einzuhalten; Führt beim Zugriff in Firmennetzwerke zu Security Risiken
Security Incidents in Form von Angriffen auf Clients haben sich in der Häufigkeit gesteigert
Maßnahme: Auslagerung von Infrastruktur (der Clients) in Cloud, um eine standardisierte Lösung über alle Benutzer zu ermöglichen. Poolressourcen genutzt

Tabelle 7: Auswirkungen auf Infrastruktur

Paraphrasen

Security und Clientmanagement bei manchen Unternehmen und Folgen nicht bewusst; Geringes Bewusstsein und keine Maßnahmen zur Absicherung haben großes Sicherheitsrisiko
Serviceerbringung hat sich geändert. User verteilt, heterogene Infrastruktur, neue Faktoren bei Servicequalität. Bestehende Services über Internet performant und Sicher. Führte zu Topologieänderungen; Auslagerung in Cloud
Cloud Services wurden implementiert. Bereitstellung über Cloud simpler als on-premise bei skalierbaren Services. Für Enduser kaum unterschied in Benutzung.
Servicequalität ausreichend verbessert
Angebot an Cloud Produkten und Lösungen steigt deutlich.
Ja, Maßnahmen mussten gesetzt werden, um Servicequalität beizubehalten
Maßnahmen: VPN für Fernzugriff wenn möglich; Ansonsten Intensivierung des Einsatzes von Cloudmodellen
Einsatz von Cloud steigert Anforderungen an Technik, Ressourceneinsatz, Wissen der IT-Mitarbeiter
Auswirkungen: Neue Herausforderungen im Umgang mit zusätzlichen Zwischenebenen im Serviceangebot (im Bezug auf Latenz, Performance)
Herausforderungen: Poolressourcen in Cloud haben Latenznachteile gegenüber on-premise Lösung.

Tabelle 8: Änderung in IT-Serviceerbringung

Paraphrasen
Maßnahme wie Awareness-Schulungen für Anwender und IT-Betrieb eingesetzt
Maßnahme: Teleworking Regelung mit Fokus auf Security. Mehr Aufkommen von Cyberangriffen
Maßnahmen zur Clientverwaltung, Netzwerksicherheit, Userschulung, Unterweisungen, Authentifizierung mit MFA
Servicequalität und Security konnte im zufriedenstellenden Maß verbessert werden;
Maßnahmen haben Servicequalität und Mitarbeiterproduktivität gefördert
Schulungsmaßnahmen, um Servicequalität beibehalten zu können. Fernzugriff große Umstellung
Maßnahmen brachten zufriedenstellende Verbesserung
Security Maßnahmen haben Einfluss auf Usability von Services (Authentifizierung, Hürden); Bringt jedoch Sensibilität von Benutzer; Maßnahmen wie Schulungen helfen
Maßnahme wie ausführliche Dokumentation hilft Usability zu verbessern
Dokumentation für unterschiedliche Devices bei Servicenutzung sinnvoll
Eigene Applikationen öffentlich anzubieten, birgt Security-Risiko; daher Tendenz eher Cloudlösung zu beanspruchen.
Maßnahme: Auslagerung von Infrastruktur (der Clients) in Cloud, um eine standardisierte Lösung über alle Benutzer zu ermöglichen. Poolressourcen genutzt
Servicequalität konnte nicht für alle Benutzer im Cloud Poolressourcen Beispiel zufriedenstellend gelöst werden, da davor teilweise on-premise Lösungen im Einsatz waren. Jedoch konnte für einige eine zufriedenstellende Lösung erreicht werden

Tabelle 9: Maßnahmen zur Einhaltung der IT-Servicequalität

7.4 Auswertung Hypothese 3

„Durch erhöhten Fokus auf den Einsatz und Adaption von Monitoringlösungen kann die Servicequalität kontinuierlich verbessert werden“

Monitoringlösungen zu betreiben bringt eine große Anzahl von Auswirkungen mit sich. Diese lassen sich auf Basis der paraphrasierten Expertenaussagen aus Tabelle 10 auf folgende Aspekte verdichten:

- Der Betrieb von IT-Infrastrukturen ohne Monitoringlösungen ist nur in kleinen Umgebungen möglich, jedoch nicht zu empfehlen. In allen anderen größeren Infrastrukturumgebungen ist der Einsatz von Monitoring für den IT-Betrieb unerlässlich
- Monitoring hilft es den Überblick zu behalten und Probleme schneller zu beheben
- Einhaltung der IT-Ziele und erhöhte Serviceerreichbarkeit konnte erreicht werden.
- Logging als Teil von Monitoring hilft Compliance mit Nachverfolgung zu schaffen.
- Standardisierung der Infrastruktur hilft Monitoring umzusetzen.
- Zeigt auf, wenn Probleme sich wiederholen und proaktiv Maßnahmen abzuleiten.
- Personal kann mithilfe von Automatismen in Monitoringsystemen entlastet werden.
- Clientmanagement wird erleichtert und Reaktion auf Sicherheitsvorfälle beschleunigt.

- Kombinationen aus on-premise Lösungen mit Cloudlösungen bringen Redundanz und Verlässlichkeit.
- Einsatz von Cloudmodellen erfordert Anpassungen bei bestehenden Monitoringlösungen oder Neukonzeption des Modells.
- Redundanzen IT-Infrastruktur nur sinnvoll wenn auch Monitoring betrieben wird.
- Auswertung und zentralisierter Überblick über Betrieb und Infrastruktur durch Monitoring erleichtert oder ermöglicht
- Implementierung soll auf Basis der Servicedefinition in Kooperation mit den Serviceownern stattfinden, um die Zielerreichung messen zu können.
- Rollentrennung von Monitoring und Fehlerbehebung.
- Monitoring bei Cloudmodellen ermöglicht flexible Ressourcenallokation.
- Monitoring verursacht Aufwände bei Personal, sowie initial und laufende Kosten.
- Zukunftsgerichtete Erweiterungen der Infrastruktur werden durch eine statistisch gegründete Historie der Leistungsmerkmale gestützt.

Paraphrasen
Monitoring ist essentiell für IT-Operations; Helfen Überblick zu erhalten sowie Probleme, Fehler und Stillstände schneller zu lösen
Monitoring hilft proaktiv statt Reaktiv zu Handeln; Unterstützt bei Anforderung von hoher Verfügbarkeit von Services
Monitoring bringt keinen Mehrwert wenn nicht aktiv gepflegt, damit gearbeitet und darauf reagiert wird.
Mehrschichtigen Monitoring im Einsatz um Serviceerreichbarkeit von intern und extern zu gewährleisten zu können
Zentrales Dashboard hilft bei Übersicht und Handhabung des Monitorings
Logging als Teil des Monitorings hilft Compliance zu gewährleisten (Nachverfolgbarkeit)
Ressourcenaufwand für Implementierung und Betreuung des Monitorings erforderte vier Personen zumindest Teilzeit
Monitoringkonzept musste adaptiert und ausgebaut werden. Security und Clientmonitoring besonderer Stellenwert aufgrund der geänderten Anforderungen.
Sicherheitskritische Themen führten zu intensivem Monitoring von Teleworking Clients. Authentifizierungsmethoden und Fernzugriff wurden angepasst
Neue Infrastruktur musste in Monitoring eingebunden werden; wurde mit Vereinheitlichung vereinfacht.
Monitoring hilft es Personal zu entlasten und Automatismen einzuführen für Überwachung, Alerting und Reporting
Monitoring hilft proaktive Maßnahmen bei wiederkehrenden Problemen zu treffen. Monitoringsystem bei Unternehmen ab mittlerer Größe unverzichtbar.
Investitionen in Monitoring forciert.
Clientmonitoring forciert; besonders mit Fokus auf Security Themen und Softwareinventarisierung. Monitoring hilft bei Security Incident Problem zu erkennen und zu beheben.
bei kleinen Infrastrukturen hat Monitoring wirtschaftlich wenig Sinn. Manuelles Monitoring praktikabler

Zu Beachten ist Grenze wann Umstellung auf automatisiertes Monitoring lohnenswert ist
on-premise Monitoringlösungen werden mit Cloudlösungen verknüpft um Redundanzen zu schaffen
Cloudmonitoringlösungen helfen auf Problemen bei on-premise Lösung hinzuweisen
Redundanzen bei Monitoring wichtig
Teleworking merklich gesteigert. Bestehende IT-Infrastruktur nicht ausreichend. Skalierbarkeit fraglich. Kapazitäten fraglich. Cloud Modelle eingesetzt. Kombination aus on-premise und Cloud erfordern angepasstes Monitoring
Monitoring essentiell um proaktiv handeln zu können
Redundante Konzepte erfordern Monitoring
Verschiedene Monitoringlösungen für Teilbereiche (Netzwerk, Security, Client, Server) und Spezialfelder sinnvoll
Monitoringlösungen erleichtern als Single-point-of-view den Überblick zu behalten. Monitoringlösungen helfen bei Auswertung und weiterführend bei Problembehebung
Serviceowner sehr wichtig. Aufgabentrennung bei Monitoring und Fehlerbehebung. Serviceowner und Servicedefinition essentiell
Enge Zusammenarbeit zwischen Serviceowner und Monitoringteam. Architektur des Monitorings muss interdisziplinär erarbeitet werden um Mehrwert daraus zu generieren
Kein Mehrwert wenn Kosten des Monitoring die Kosten die Kostenersparnis im Betrieb übersteigen. Monitoring erzeugt Kosten bei Personal, Hardware, Lizenzierung.
Kunden sehen bei Monitoringkonzeption bereits ob der Mehrwert den Ressourcenaufwand für die Implementierung gerechtfertigt
Proof-of-Concept hilft für Kunden ein Verständnis für die Wichtigkeit des Monitorings zu schaffen
Cloud Service Modelle ermöglichen in Kombination mit Monitoring flexible Ressourcenbereitstellung. Ermöglicht Services bei sich ändernden Anforderungen automatisiert mitzuskalieren. On-Premise Infrastruktur erfordert Initialinvestition, Cloud nicht.
Auswirkung: Teleworking erfordert umfangreicheres Monitoring; weil schwerer zu erreichen und schwerer Fehler zu beheben
Monitoringlösungen essentiell für IT-Betrieb
Kennzahlen für Monitoring wie Auslastung, Erreichbarkeit, Security Incidents sehr wichtig für Betrieb. Monitoringlösungen helfen dabei diese zu ermitteln.
Kein Grund ersichtlich wieso Monitoringlösungen keinen Mehrwert bringen
Monitoring ermöglicht Administration zu erleichtern; zeigt den Zustand der betrachteten Systeme, deren Performance und Probleme mittels Statistiken
Kundenanforderungen haben sich im Hinblick zum Umfang und Fähigkeiten der Monitoringlösungen erweitert mit Blick auf zukünftige Infrastruktur Erweiterungen.

Tabelle 10: Einsatz von Monitoring(lösungen)

Auf Basis der Paraphrasen der Tabelle 11 können Kennzahlen für Monitoring auf Themengebiete aus der folgenden Auflistung zusammengefasst werden:

- Sicherheit
    - Authentifizierung
    - Compliance (für den Zugriff auf das interne Netzwerk oder Organisationsdaten)
- Logging in Hinblick auf Nachverfolgbarkeit
- Einsatz und Einbindung von Cloudmodellen
- Netzwerkmonitoring (Latenz bei Einsatz von Cloudressourcen)
- Clientmanagement

  - Softwarebereitstellung
  - Updateverteilung
- Performancemanagement der Servicedefinition von Serviceownern

Paraphrasen

Sicherheitskritische Themen führten zu intensivem Monitoring von Teleworking Clients. Authentifizierungsmethoden und Fernzugriff wurden angepasst
Clientmonitoring forciert; besonders mit Fokus auf Security Themen und Softwareinventarisierung. Monitoring hilft bei Security Incident Problem zu erkennen und zu beheben.
Teleworking merklich gesteigert. Bestehende IT-Infrastruktur nicht ausreichend. Skalierbarkeit fraglich. Kapazitäten fraglich. Cloud Modelle eingesetzt. Kombination aus on-premise und Cloud erfordern angepasstes Monitoring
Verschiedene Monitoringlösungen für Teilbereiche (Netzwerk, Security, Client, Server) und Spezialfelder sinnvoll
Monitoringlösungen erleichtern als Single-point-of-view den Überblick zu behalten. Monitoringlösungen helfen bei Auswertung und weiterführend bei Problembehebung
Enge Zusammenarbeit zwischen Serviceowner und Monitoringteam. Architektur des Monitorings muss interdisziplinär erarbeitet werden um Mehrwert daraus zu generieren
Cloud Service Modelle ermöglichen in Kombination mit Monitoring flexible Ressourcenbereitstellung. Ermöglicht Services bei sich ändernden Anforderungen automatisiert mitzuskalieren. On-Premise Infrastruktur erfordert Initialinvestition, Cloud nicht.
Kundenanforderungen haben sich im Hinblick zum Umfang und Fähigkeiten der Monitoringlösungen erweitert mit Blick auf zukünftige Infrastruktur Erweiterungen.
Investitionen in Ressourcen für Monitoring gestiegen. Cloud und On-Premise Monitoring unterschiedlich zu monitoren.
Monitoring wurde Richtung Security für Infrastruktur und Services forciert.
Für Cloud Service Modelle ist Monitoring anders umzusetzen, meist mit Schnittstellen des Betreibers.
Services werden Komplexer zu monitoren wenn Infrastruktur heterogener wird.
Clientverwaltung, Update Compliance, Software Compliance sind aufgrund der heterogenen Umgebungen schwerer geworden einzuhalten; Führt beim Zugriff in Firmennetzwerke zu Security Risiken
Auswirkungen: Neue Herausforderungen im Umgang mit zusätzlichen Zwischenebenen im Serviceangebot (im Bezug auf Latenz, Performance)
Herausforderungen: Poolressourcen in Cloud haben Latenznachteile gegenüber on-premise Lösung.
Anforderungen an Monitoring ändern sich im Hinblick auf reinem IT-Infrastruktur Monitoring zu ganzheitlichen Servicemonitoring mit Integration von Cloud Modellen
Security Monitoring hat an Bedeutung enorm gewonnen

Tabelle 11: Monitoringkennzahlen

8 CONCLUSIO

Der Einsatz von Teleworking Arbeitsplätzen ist seit dem Beginn der Pandemie von COVID-19 ein beliebtes Mittel in der Infektionseindämmung innerhalb von Organisationen. Der vermehrte Einsatz dieser spezifischen Art von Arbeitsplätzen, teils auch nicht ausreichend vorbereitet, birgt auch negative Auswirkungen auf die IT-Infrastruktur der Organisation selbst. Zudem können die sich geänderten Anforderungen auch auf die Architektur von Monitoringsystemen sowie den darin festgelegten Kennzahlen haben. Die IT-Infrastruktur kann als das Rückgrat aller angebotenen IT-Services angesehen werden. Aus diesem Grund gilt es hier besonderes Augenmerk zu legen.

Die Forschungsfrage dieser Arbeit lautet:

„Wie haben sich mit vermehrtem Einsatz von Teleworking Arbeitsplätzen in der Pandemie von COVID-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert?“

Es kann auf Basis der Auswertung abgeleitet werden, dass sich die Anforderungen an Monitoring Kennzahlen im Hinblick auf erforderliche (neue) Maßnahmen zur Einhaltung dieser und Zusammensetzung der Kennzahlen selbst verändert haben.

Auf Basis der gewonnen Erkenntnisse haben sich folgende geänderte Anforderungen an Monitoring Kennzahlen für IT-Operations ergeben:

- Sicherheitskennzahlen
    - Authentifizierung
    - Compliance (für den Zugriff auf das interne Netzwerk oder Organisationsdaten)
        - Hierbei war auf Basis der Auswertung wichtig, mit den Unternehmensrichtlinien sowie Sicherheitsrichtlinie abgestimmte Kennzahlen zu definieren (wie der Authentifizierungsmodalität). Zudem war es wichtig, die Compliance hinsichtlich der Nachweispflicht mithilfe eines Logging Konzepts gewährleisten zu können. Die Kombination dieser Kennzahlen für das Monitoringsystem können Anforderungen seitens der Erhöhung der Sicherheit und Compliance erfüllen.
- Einsatz und Einbindung von Cloudmodellen
    - Die Erweiterung von Monitoring für den Einsatz von Cloud Modellen und deren individuellen Schnittstellen hilft es, neu hinzugekommene und ausgelagerte Infrastruktur im gleichen Maß überwachen zu können.
- Netzwerkmonitoring (in Hinblick auf Latenz bei Einsatz von Cloudressourcen)
    - Ein weiterer wichtiger Punkt ist es, die speziellen Anforderungen der Netzwerkinfrastruktur in Kombination mit Teleworking Arbeitsplätzen einzubinden. Hierbei wurde in der Auswertung speziell Kennzahlen wie Latenz beim Zugriff auf Ressourcen im und außerhalb vom Netzwerk und VPN Bandbreite aufgeführt.

    - Zusätzlich ist es sinnvoll, Netzwerkverkehr nach Art und Typ zu monitoren, um eine Priorisierung vornehmen zu können.

- Clientmanagement
    - Softwarebereitstellung, Updateverteilung
    - Das Clientmanagement wurde aufgrund der verteilten Infrastruktur der Clientendgeräte erschwert. Diese Erschwernis konnte mithilfe von Monitoring der Softwarebereitstellung und Updateverteilung abgemildert werden. Kennzahlen dieser Eigenschaften können beispielsweise das Datum des letzten Updatezyklus, installiertes Softwareupdate und Version dieser sein. Je detailreicher diese Überwachung ist, desto hilfreicher ist es für die IT-Organisation im Sinne der Fehlerbehebung.
- Performancemanagement auf Basis der Servicedefinition von Serviceownern
    - Serviceowner sollen für die Definition und Ausformulierung der Servicekataloge und dem Monitoring eingebunden werden. Je enger die interdisziplinäre Zusammenarbeit der Abteilungen und Teams ist, desto höher der Mehrheit für die Servicebereitstellung. Jeder Fachbereich hat individuelles Domänenwissen und kann dies mit dem bestehenden Wissen über Teil der betreuten Infrastruktur kombinieren und das Monitoring zielgerichtet verbessern. Die Einbindung hat, sofern seitens der Organisation Serviceowner definiert wurden, erhöht und bringt großen Mehrwert.

Es hat sich auch abgezeichnet, dass für Organisationen das Thema Monitoring als Ganzes wichtiger wurde und wesentlich dabei geholfen hat, die IT-Infrastruktur und Servicelandschaft zu betreiben. Besonders der Hintergrund sich vor Sicherheitsvorfällen zu schützen hat neue Anreize geschaffen.

Abschließend kann festgehalten werden, dass die gewonnen Erkenntnisse aus der vorliegenden Untersuchung die Fragestellung erfolgreich beantworten.

9 AUSBLICK

Das Ziel dieser Arbeit war es zu beleuchten, wie sich Teleworking, als teils ruckartige und signifikante, Umstellung innerhalb von Organisationen in der Arbeitsplatzeinbindung auf die IT-Infrastruktur und den dazugehörigen Monitoringsystemen und Kennzahlen auswirkt.

Darauf kann seitens Experten für Monitoringlösungen noch aufgebaut werden, welche Kennzahlen sich im speziellen eignen, um ein Monitoringsystem zur Unterstützung vom Clientmanagement innerhalb von Organisationen zu implementieren. Diese Auswahl an Kennzahlen kann dann als Katalog verdichtet dargelegt werden.

Die Grenzen dieser Arbeit liegen in der detaillierten Erhebung von einzelnen Monitoringkennzahlen und ihrer Bedeutung im Kontext von Teleworking Arbeitsplätzen. Dies würde sich jedoch auch als weiteres Forschungsthema anbieten, um die Auswirkungen vom Einsatz dieser Art von verteilten Arbeitsplätzen auf die Kennzahlen selbst bestimmen zu können.

Im Umgang mit großen und komplexen Datenmengen (Big Data) wie es bei Monitoringkennzahlen der Fall ist, wäre auch eine Auswertung mittels Machine Learning Algorithmen zu untersuchen und zu testen. Aufbauend auf diesen Algorithmen kann evaluiert werden, inwiefern diese helfen können verdächtige Aktivitäten oder irreguläres Verhalten aufzudecken und proaktiv Maßnahmen vorschlagen oder einleiten zu können. Weiters wäre es sinnvoll bei sich wiederholenden Anomalien von Kennzahlen, darauf hinzuweisen wie sich Kennzahlen bis zum Auftreten dieser verändern.

ANHANG A - Leitfaden Experteninterview

Kategorie	*Nr*	*Einleitung/Fragestellung*
Einleitung	0	Vorstellung Thema und Forschungsfrage
Einleitungsfragen	1	Wie viele Jahre haben Sie bereits Erfahrung mit Monitoringlösungen für IT-Infrastruktur sammeln können?
Einleitungsfragen	2	Wie viele Jahre haben Sie bereits Erfahrung in Betreuung, Administration oder Projektmitarbeit von IT-Infrastruktur sammeln können?
Einleitungsfragen	3	Bei wie vielen Kunden waren, sie in der Administration, Betreuung oder Projektmitarbeit von IT-Infrastruktur beteiligt?
Einleitungsfragen	4	Mit welchen Monitoringlösungen konnten Sie bereits Erfahrungen sammeln?
Hypothese 1	5	Hat sich im Rahmen der Pandemie von COVID-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?
Hypothese 1	6	Wie haben sich Aufgrund des vermehrten Einsatzes von Teleworking Anforderungen an die IT-Infrastruktur geändert?
Hypothese 1	7	Wie haben sich diese Änderungen der Anforderungen an die Infrastruktur ausgewirkt?
Hypothese 2	10	Hat der vermehrte Einsatz von Teleworking Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Serviceumgebungen?
Hypothese 2	11	Falls ja, wie haben sich diese Auswirkungen bemerkbar gemacht?
Hypothese 2	12	Mussten Aufgrund dieser wandelnden Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Servicequalität beibehalten zu können?
Hypothese 2	13	Wenn ja, welche Maßnahmen wurden gesetzt?
Hypothese 2	14	Haben diese Maßnahmen die Servicequalität in zufriedenstellenden Maß die Servicequalität verbessert?
Hypothese 3	15	Inwiefern helfen Monitoringlösungen den laufenden Betrieb von IT-Services und Infrastruktur zu unterstützen?

Hypothese 3	16	Gibt es Fälle, in denen der Einsatz von Monitoringlösungen keinen Mehrwert bringt? a. Welchen Grund hat dies?
Abschließende Fragen	17	Wie haben Sie das Interview empfunden?
Abschließende Fragen	18	Haben Sie noch Anmerkungen zu den Fragen?
Abschließende Fragen	19	Haben Sie noch zusätzlichen Input zum Forschungsthema?

ANHANG B - Experteninterview Person 1

Speaker 0 Das sollte jetzt funktionieren. Also lieber Experte 1. Wie Willkommen zum Experteninterview zum Thema Kennzahlen im Kontext des Infrastruktur Monitorings. Beginnen wir mal bei der Übersicht. Also ich erklär Ihnen jetzt kurz mal am Anfang die Forschungsfrage. Dann kommen wir zur Einleitung bzw. Einleitungsfragen, dann zu den Frageblöcken 1 bis 3 und den Abschlussfragen, falls es noch offene Fragen oder Beanstandungen gibt.

Die Forschungsfrage lautet "Wie haben sich mit vermehrtem Einsatz von Teleworking Arbeitsplätzen in der Pandemie von Covid-19 die Anforderungen an Monitoring Kennzahlen für IT Operations verändert". Nun kommen wir zu den Einleitungsfragen. Also, lieber Herr Experte, wie viele Jahre haben Sie bereits Erfahrung mit Monitoring Lösungen für IT-Infrastruktur sammeln können?

Speaker 1 Gute Frage. Wenn ich jetzt so zurückrechne für unser Auge mal Pi bis dato in Bezug auf Monitoringlösungen ungefähr 9 Jahre Erfahrung.

Speaker 0 Und wie viele Jahre haben Sie bereits Erfahrung in der Betreuung Administration oder Projekt Mitarbeit von IT-Infrastruktur sammeln können?

Speaker 1 Dort dürften es relativ genau in Summe bereits elf Jahre sein.

Speaker 0 Okay, bei wie vielen Kunden waren Sie in der Administration, Betreuung oder Projektmitarbeiter von IT-Infrastruktur beteiligt?

Speaker 1 Ähm, ja, also grundsätzlich ich persönlich bin bis dato immer in der internen IT angesiedelt gewesen und habe mich um interne Projektleitung interne Infrastruktur gekümmert überwiegend. Von dem her quasi in diesem Fall die drei eigenen Firmen, bei denen ich gearbeitet habe und bei anderen Firmen eher indirekt durch Erfahrungsaustausch mit Kollegen.

Speaker 0 Und noch abschließend jetzt von der Einleitung. Mit welchen Monitoring Lösungen konnten Sie bereits Erfahrungen sammeln?

Speaker 1 Mittlerweile doch mit der einen oder anderen Lösung. Ähm, also konkret hatte ich bereits Nagios im Einsatz, auch von WürthPhoenix die NetEye, welche auch auf der Basis von Nagios läuft, als auch mit PRTG. Im Moment beschäftige ich mich mit Zabbix fürs interne Monitoring upRobot fürs externe Monitoring und im Moment auch mit den Lösungen Splunk und Elasticsearch in Bezug auf Logging

Speaker 0 okay, dann beginnen wir mit dem ersten Frage Block. Und zwar hat sich im Rahmen der Pandemie von Covid-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?

Speaker 1 Gute Frage und ich glaube, die Frage lässt sich klar mit einem Ja beantworten. Grundsätzlich hängt es natürlich stark vom Berufsfeld und von der Branche bzw. der Rolle der Person ab, ob sie Teleworking überhaupt machen kann oder nicht. Ich sage mal, ein Verkaufs Mitarbeiter zum Beispiel beim Spar; bei dem wird es schwierig sein Teleworking zu betreiben. Wobei ich auch hier bereits erlebt habe, dass vorallem in solchen Branchen begonnen wurde, zum Beispiel Schulungen online durchzuführen. Aber bei Personen, die überwiegend im Büro tätig sind und vor allem auch in der IT-Branche gab es einen riesigen Umbruch bzw. wird sehr viel Teleworking mittlerweile betrieben bzw. wird auch mehr und wird auch großteils so bleiben.

Speaker 0 Die zweite Frage ist "Wie haben sich aufgrund des vermehrten Einsatzes von Teleworking die Anforderungen an die IT-Infrastruktur geändert?"

13 Speaker 1 Also grundsätzlich ist es eine Frage, die sich leider viel zu wenige Unternehmen stellen. Meiner Meinung nach wird, so aus dem Bauch heraus beantwortet, zählt dazu auf jeden Fall, dass das Unternehmen zeitgemäße und gut gewartete Firewalls haben, das für Teleworking, je nachdem wo es genau geht, VPN Clients im Einsatz sind und zwar ohne Split-Konfiguration, so dass quasi wirklich über den gesicherten Kanal die Daten gehen, dass eventuell das Netzwerk Design neu überdacht werden muss, vor allem in Bezug auf wo darf man von wo aus hin und wo nicht. Ein Thema dahingehend sind sich auch Awareness-Schulungen sowohl für die IT Mitarbeiter selbst als auch für die Mitarbeiter außerhalb der IT. Ein Thema das sich erlebt habe, dass da auch immer wieder schlagend wurde in letzter Zeit ist die Internetanbindung aufgrund von steigenden Traffic eben durch VPN daher sollte natürlich auch entsprechende Internetanbindung vorhanden sein. Und ganz wichtig, es muss eine klare Regelung zum Thema Telearbeit im Unternehmen geben. Wichtig sind vor allem auch im Bezug auf die Sicherheit. Vor allem, weil es in letzter Zeit vermehrt, also wirklich eigentlich viel mehr, als wie noch vor ein bis zwei Jahrenn zu Cyberangriffen kommt.

14 Speaker 0 Okay, die dritte Frage "Wie haben sich diese Änderungen der Anforderungen auf die Infrastruktur ausgewirkt? "

15 Speaker 1 Also grundsätzlich würde ich sagen, dass sich all diese Änderungen in Form von Sicherheit positiv auf die Infrastruktur ausgewirkt haben, im Sinne von dass das Unternehmen einfach im Sinne der Sicherheit mehr profitiert und sich selbst damit absichert und schützt. Und zum anderen wurde dadurch meiner Meinung nach auch die Servicequalität einfach erhöht. Es gibt bessere Verfügbarkeit, mehr Flexibilität und mehr Sicherheit, ohne dass die User quasi unter großen Einschränkungen leiden.

16 Speaker 0 Okay, sehr gut. Das zweite Block, Die erste Frage "Hat der vermehrte Einsatz von Teleworking Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Service Umgebungen?

17 Speaker 1 Ähm ja, also negative Auswirkungen ist jetzt relativ. Ich sag mal, bei fehlender Vorbereitung bzw. einer schwach aufgestellten IT-Infrastruktur gibt es natürlich negative Auswirkungen, wie zum Beispiel Services fallen aus, die Verfügbarkeit ist eingeschränkt und vieles mehr. Aber ich glaube, der Hauptpunkt ist momentan wirklich und dass vielen Unternehmen nicht bewusst das Thema Security und durch fehlendes Clientmanagement kann halt recht schnell und durch schwache Infrastruktur und schwache Absicherungen, zu wenig Budget, alten Firewalls etc. wirklich zu gravierenden Problemen in der Infrastruktur kommen, bedingt durch Cyberangriffe etc..

18 Speaker 0 Ok, damit haben wir die zweite Frage auch direkt mitbeantwortet, dann zur ditten Frage und zwar "Mussten aufgrund dieser wandelnden Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Servicequalität beibehalten zu können? Und wenn ja, welche Maßnahmen wurden gesetzt?

19 Speaker 1 Also grundsätzlich waren wir im Unternehmen nicht so schlecht aufgestellt was das betrifft, da bei uns auch Teleworking und Telearbeit zuvor auch schon gelebt wurde. Aber trotz dessen gab es natürlich bestimmte Optimierungen und Lösungen wie organisatorische und technische Themen. Ja, welche Maßnahmen wurden gesetzt? Unter anderem wurde zum Beispiel die Updateverwaltung der Clients geändert. Firewall Regeln wurden nachgeschärft. Es gibt neue Awareness-Schulungen und Unterweisungen für bestimmte Applikationen, damit das einfach flüssiger funktioniert und sicherer ist. Gibt es oder werden im Moment Terminalserver eingesetzt. Es wurde uns also quasi mit der Zeit zu gehen eine Multi-Faktor-Authentifizierung eingeführt und vieles mehr.

20 Speaker 0 Und fünfte "Frage Haben diese Maßnahmen die Servicequalität in zufriedenstellenden Maß verbessert?"

Speaker 1 Also Ja, also ich sage grundsätzlich wir haben es dadurch geschafft, die IT Sicherheit dadurch zu erhöhen, aber sowie auch die Verfügbarkeit und die Servicequalität ohne großartig irgendwelche Einschränkungen und Mehraufwand bei den Mitarbeitern zu erzeugen. Da ein Ziel natürlich immer ein hohes Maß an Servicequalität war und dass die Produktivität der Mitarbeiter durch Lösungen auch nicht eingeschränkt wird, sondern im Idealfall sogar noch gefördert wird. Also ja, die Maßnahmen haben definitiv zur Servicequalität beigetragen.

Speaker 0 Dann sind wir schon beim dritten Block. "Inwiefern helfen Monitor und Lösungen, den laufenden Betrieb von IT Services und Infrastruktur zu unterstützen?"

Speaker 1 Meiner Meinung nach sind hier einfach essenziell für die IT Abteilung. Ist natürlich auch immer ein bisschen abhängig von der Größe der Unternehmen, um den Überblick zu behalten, um auf Probleme, Fehler und Stillstände schneller reagieren zu können. Um ein Gesamtbild zu erhalten und dadurch auch Fehler eingrenzen zu können. Und im Idealfall anstatt reaktiv, wenn schon bereits was eingetreten ist, vielleicht präventiv, bevor etwas eintritt, Maßnahmen einzuleiten, so dass man sich den Ausfall spart, die Verfügbarkeit erhöht, die Servicequalität gesteigert wird, wie im Sinne von Hausnummer eine Festplatte läuft irgendwo auf einem Server voll. Es droht quasi ein Stillstand, weil eine Datenbank drauf ist. Und durch entsprechendes Monitoring zum Beispiel könnte man schon vorab reagieren und sieht die Platte nähert sich dem Limit und kann dann entsprechend quasi agieren und eingreifen, den Stillstand verhindern.

Speaker 0 Dann zur zweiten Frage "Gibt es Fälle, in denen der Einsatz von Monitoren Lösungen keinen Mehrwert bringt? Und wenn ja, welchen Grund hat es? "

Speaker 1 Ja, also ein eindeutiges Ja aus meiner Sicht. Aber ich habe es mittlerweile leider zu oft erlebt, also selbst erlebt, und auch bei anderen erlebt, dass die IT-Infrastruktur mehr als quasi Kosten gesehen werden im Unternehmen als auch das, was sie wirklich erbringen kann. Und in dem Sinne gab es dann oft zu wenig Budget, zu wenig Zeit bzw. Ressourcen im Sinne von Personal. Aber es gibt dann quasi ein Monitoring, dieses Monitoring ist aber halbfertig, nicht gepflegt oder wird nur so nebenbei betrieben. Und so ein Monitoring ist quasi im Prinzip, sofern es zum Beispiel nicht auf freier Basis ist und auch noch Lizenzkosten dazukommen, Geldverschwendung, weil im Regelfall, wenn etwas passiert, wird genau das nicht gemonitored, oder andersherum es wird zwar gemonitored aber keiner reagiert, weil keiner hingeschaut hat, weil fehlende Zeit, zu viele Meldungen immer kamen, weil schlecht gewartet und so weiter und so fort. Also ja, wenn zu wenig Zeit, Budget und Ressourcen da sind, dann aber hat man auch keinen Mehrwert durch eine Monitoringlösung.

Speaker 0 Okay, das klingt ein Mal sehr interessant. Dann zum Abschlussblock. Wie haben Sie das Interview empfunden?

Speaker 1 Ja, es ist sehr angenehm. Ich finde das Thema, die Forschungsfrage sehr spannend. Ich finde, dass das sehr wichtiges Thema ist und mir gefällt die Frage besonders gut, weil ich glaube, dass ich diese Frage erstens sehr, sehr wichtig ist und zweitens leider glaube ich viel zu wenige Personen oder Unternehmen überhaupt aus dieser Sicht das Ganze betrachten. Vor allem jetzt im Zuge von Corona und und Teleworking. Tolles Thema und finde ich spitze, dass das im Rahmen einer Masterarbeit erörtert wird.

Speaker 0 Und haben Sie noch weitere Anmerkungen zu den Fragen?

Speaker 1 Im ersten Moment eigentlich nicht.

Speaker 0 NHaben Sie eventuell noch zusätzlichen Input zum Forschungsthema?

31	Speaker 1	Vielleicht als Input oder als Ergänzung, ist grundsätzlich find die Betrachtung sehr spannend und ich glaube, dass zu wenige Unternehmen seine Betrachtung durchführen. Und ganz essenziell in die Richtung ist aber auch immer nicht nur diese technische Betrachtung, oft scheitert es gar nicht nur an, wie soll ich das am besten formulieren? Oft scheitert es quasi nicht nur daran, dass sich Firmen nicht bewusst sind, sondern oft scheitert es auch quasi eine Bewusstseinsbildung, dass eigentlich die IT-Infrastruktur mehr oder weniger das Rückgrat des Unternehmens darstellt und bei dem Beispiel schlechter Absicherung, vermehrten Working und einem Cyberangriff ist leider vielen zu wenig bewusst, dass wenn man sich genau diese Frage nicht stellt, das Unternehmen innerhalb von wenigen Minuten vom Erdboden verschwunden sein kann. Das ist quasi so einen Schwank drumherum. Aber es hat jetzt nicht nur die technische Betrachtung in Bezug auf Kennzahlen, sondern grundsätzlich glaube ich sie dahingehend auch das Thema überhaupt Bewusstseinsbildung und IT-Aufstellung der Infrastruktur im Unternehmen glaube ich sehr breit gefächertes Thema.
32	Speaker 0	Ich hätte eventuell noch eine zusätzliche Frage Was ist denn bei Ihnen im Unternehmen aktuell, zumindest grob umrissen, die Monitoringlösung ausgerollt bzw. aufgebaut?
33	Speaker 1	Ähm, also wir sind im Moment dabei, eine alte Lösung abzulösen, die irgendwie wie vorhin erwähnt leider schlecht gepflegt wurde oder nur ja ich sage mal zwar da war, aber nicht wirklich einen Mehrwert gebracht hat. Die wird jetzt zum einen durch drei Lösungen im ersten Schritt abgelöst, zum einen durch Zabbix und dann verwendet für fürs interne Monitoring im Unternehmen, also für Server Netzwerk Switches im Sinne von Basis Monitoring wie Disk Space, gibt es irgendwo Hardwaredefekte etc. Dann gibt es das große Thema, also auch die Außensicht. Es hilft nichts, wenn ihr nur von ihnen sehe, ist der Webserver da. Aber die Website ist eigentlich von außen nicht erreichbar, weil irgendwo anders zum Beispiel ein Problem gibt. Da bauen wir gerade im Moment zusätzlich mit der Uptimerobot ein Monitoring auf. Das ist ein Cloud Service, den man zusätzlich auch mieten kann, wo man nach Sensoren zahlt, wo man zum Beispiel auch die Außensicht auf einfache Art und Weise mitprüfen kann. Wir haben da auch mittlerweile mehrere Monitore quasi im IT-Büro und an den Standorten mit Lösungen gebastelt wo ein Dashboard drauf ist mit Überblick der Lösungen, so dass quasi nicht die getrennten Lösung anzuschauen sind, sondern alles auf einen Blick und zusätzlich auch in Bezug auf TISAX, diese Zertifizierung in Bezug auf IT-Sicherheit und Unternehmenssicherheit für die Automobilbranche und auch in Bezug auf die ISO 27001 ist ein großes Thema, das Logging, wo wir jetzt aber zusätzlich versuchen und da ist das Thema elkstack/elasticsearch oder Splunk Logs zu analysieren, um uns auch da besser aufzustellen, weil Hausnummer sollte der Cyber-Angriffen Unternehmen stattfinden dann gibt es vermutlich bevor das oder bevor die IT-Abteilung das im Regelfall merkt, gibt schon verschiedenste Anzeichen dafür. Und deswegen sind auch bei diesen Zertifizierungen die Prüfer auch dahinter, dass das entsprechende Logging gibt, weil man dadurch einfach, wenn man es sinnvoll betreibt, einen Schaden abwenden oder im Fall des Falles erheblich reduzieren kann und die Service Qualität steigern kann, indem man dann eigentlich erst darauf kommt, welche anderen Probleme und Themen sonst noch so im Netz herumschwirren, die man sonst gar nicht so richtig bemerkt bzw. dadurch wird natürlich auch wenn genauere Analysen im Netzwerk Bereich und so weiter und sofort möglich. Also Logging ist ein ganz mächtiges Thema.
34	Speaker 0	Okay, das klingt sehr, sehr spannend und umfangreich. Die implementierte Kombination von den Lösungen
35	Speaker 1	ja, passt, aber das Gesamtpaket schlussendlich bringt quasi entsprechenden Mehrwert und dadurch den Aufwand auch in
36	Speaker 0	Haben Sie noch einen Einblick oder können Sie einen Blick auf das überschlagen, wie viel Ressourcen und Personal für die Umsetzung aufgewendet werden?

37	Speaker 1 Ähm. Also im Moment ist das Projekt lauft das Projekt schon eine Zeit lange. Wir fahren da diesen agilen Ansatz, wir machen so quasi immer wieder kleine Arbeitspakete, die man dann einer in einem Sprint einfach umsetzen und wir schauen dann, wo wir sind und entsprechend ergeben sich neue Themen und so hanteln wir uns fort, damit man auch wirklich Lösungen bekommt, die quasi jetzt nirgendwo in Stein gemeißelt ist, sondern die uns auch wirklich was bringt und ab und zu kommt man jetzt einen gewissen Zeitpunkt darauf. Okay, das war jetzt vielleicht die falsche Richtung. Dann müssen wir noch irgendwie einlenken und im Moment arbeiten vier Personen daran.
38	Speaker 0 Okay, okay, sehr interessant. Dann bedanke ich mich für das Interview und wünsche Ihnen noch weiterhin alles Gute.
39	Speaker 1 Ja, danke! Viel Erfolg mit Ihrer Masterarbeit.

ANHANG C - Experteninterview Person 2

1	Speaker 0 Also lieber Herr Experte, willkommen zum Experten Interview für mein Forschungsthema mit der mit der Überschrift "Kennzahlen im Kontext des Infrastuktur Monitorings". Beginnen wir mal mit der Übersicht. Und zwar beginnen werden wir jetzt mit der Forschungsfrage, damit Ihnen das natürlich deutlicher wird, um was es genau beim Thema geht. Dann gehen wir über zur Einleitung bzw. den Einleitungsfragen. Dann fahren wir fort mit den Frageblöcken 1 bis 3 und werden das ganze abschließen mit ein paar Abschlussfrage und eventuellen Ergänzungen von Ihnen. Nun zur Forschungsfrage "Wie haben sich mit vermehrten Einsatz von Teleworking Arbeitsplätzen in der Pandemie von Covid-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert?" Nun zur ersten Einleitungsfrage Wie viele Jahre haben Sie bereits Erfahrung mit Monitoringlösungen für IT-Infrastruktur sammeln können?
2	Speaker 1 Ja, mittlerweile bin ich seit sechs Jahren mit Monitoringlösungen in der IT vertraut und habe bereits Erfahrungen damit gesammelt und auch implementiert und betreut.
3	Speaker 0 Okay, wie viele Jahre haben Sie bereits Erfahrung in der Betreuung, Administration oder Projektmitarbeit von IT-Infrastruktur sammeln können?
4	Speaker 1 Das sind mittlerweile zehn Jahre lang, angefangen von Second Level bis Third-Level.
5	Speaker 0 Okay, bei wie vielen Kunden waren Sie in der Administration Betreuung oder Projektmitarbeit von IT-Infrastruktur beteiligt?
6	Speaker 1 Da ich in einem Consulting Unternehmen tätig bin, sind es mittlerweile über 30-40 Kunden, wo ich aktiv an Projekten beteiligt war und umgesetzt habe.
7	Speaker 0 Okay. Und nun zur letzten Einleitungsfrage. Mit welchen Monitoringlösungen konnten Sie bereits Erfahrungen sammeln?
8	Speaker 1 Dabei gibt es eigentlich drei große Monitoringsysteme, mit denen ich bereits gearbeitet habe. Das wäre zum einen SCOM, zum zweiten Nagios und zum dritten PRTG.
9	Speaker 0 Nun beginnen wir mit dem ersten Frage Block und mit der ersten Frage. Hat sich im Rahmen der Pandemie von COVID-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?
10	Speaker 1 Ja, was wir feststellen konnten, ist, dass natürlich die Anfrage an mobilen Geräten, die speziell auch für den Home-Office Betrieb ausgelegt waren, deutlich vermehrt haben. Da ist es auch zu Anfang zu Engpässen gekommen im Rahmen der Bestellungen und in der Auslieferung. Also dieser Punkt wurde sehr deutlich klar, dass hier der Fokus drauf gesetzt wurde.
11	Speaker 0 Zweitens: Wie haben sich aufgrund des vermehrten Einsatzes von Teleworking die Anforderungen an die IT-Infrastruktur geändert?
12	Speaker 1 Natürlich aufgrund des Einsatzes der Teleworking Stationen mussten teilweise Firewalls neu ausgestattet werden, vergrößert werden, mehr Lizenzen angeschafft werden. Es mussten mehr Arbeitsplätze quasi in den Homeoffice Betrieb verlegt werden, und die IT-Infrastruktur dahingehend vergrößert werden, indem man selber Terminalserver Farmen installiert hat, bereitgestellt hat für die Arbeitskräfte, die vom Homeoffice aus gearbeitet hat. Ja und natürlich auch die Securitykonzepte müssen hier ganz stark adaptiert werden, da sich der Zugriff natürlich vom Homeoffice in die Firmen Infrastruktur hier sehr viele Graubereiche aufgedeckt haben welche nach und nach gestopft werden mussten hinsichtlich Security.
13	Speaker 0 Damit haben wir eigentlich auch schon die dritte Frage beantwortet. Könnten Sie Beispiele aufzählen, was sich dann geändert hat bzw. was angepasst werden musste?
14	Speaker 1 Genau da ging es dann um so Themen wie Authentifizierungsmethoden und MFA zum einen, zum anderen eben Firewalltechnisch. Was wird hier alles geloggt, von wo aus melden sich mobile Clients an. Wartungstechnisch, sind diese Clients immer

up to date, sind korrekt mit dem Unternehmen und mit Unternehmensinfrastruktur verknüpft. Gibt es hier irgendwelche Schlupflöcher, wo sich die Clients befinden. Das zusammen musste dann auch mit dem Monitoringkonzept überarbeitet werden, damit hier ein stimmiges Bild gebaut werden konnte zwischen all den Bereichen.

15 Speaker 0 So, dann fahren wir jetzt fort mit dem zweiten Frage Block Mit der ersten Frage: Hat der vermehrte Einsatz von Teleworking Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Service Umgebungen?

16 Speaker 1 Hier würde ich eher die positiven Aspekte in den Vordergrund stellen. Negative Auswirkungen dahingehend, dass viele Unternehmen kurzfristig mit der Situation überfordert waren, da hier doch einige Punkte quasi aufgedeckt wurden, die bisher eher stiefmütterlich bis gar nicht beachtet wurden. Und durch die neue Situation von COVID-19 hat sich das natürlich geändert und hier wurden dann einige kritische Themen aufgerollt und konnten umgesetzt werden und angepasst werden und letztlich die Infrastruktur im gesamten verbessert hat.

17 Speaker 0 Okay, das klingt sehr interessant. Dann kommen wir zu der zweiten Frage "Falls ja, wie haben sich diese Auswirkungen bemerkbar gemacht? Könnten Sie dort ein Beispiel, ein spezifischeres anführen?

18 Speaker 1 Zum Beispiel war es früher möglich, dass man mit einem Laptop von zu Hause aus sich ungesichert ins Firmennetz verbinden hat können mittels simpler VPN Möglichkeiten. Mittlerweile braucht man hierzu auch MFA, eine 2-Faktor-Authentifizierung. Das Gerät ist immer überwacht durch Intune oder andere O365 Lösungen implementiert wurden und somit ist hier auch eine dauerhafte Monitoring Lösung auf den Home Office Geräten implementiert worden. Das hat es früher so nicht gegeben.

19 Speaker 0 Okay, sehr interessant. Dann zur dritten Frage: Mussten aufgrund dieser wandelnden Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Servicequalität beibehalten zu können?

20 Speaker 1 Ja, es mussten zum Einen natürlich viel mehr aufeinander abgestimmte mobile Geräte angeschafft werden. Viele Firmen hatten früher einen ein riesen Konvolut an Hardware, an Geräten, an verschiedenen Laptops und Hersteller. Dies würde es alles eher vereinheitlicht um eben auch für das Monitoring dahinter, welches auch nicht ganz simple ist, möglichst wenig Aufwand zu generieren, um alle Systeme abdecken zu können. Zum einen musste das Ganze dann auch erstmal in das Monitoring eingebunden werden, was natürlich auch entsprechend umgesetzt werden musste. Dann mussten die User geschult werden. Speziell da der Einsatz von VPN und mobilen Geräten viele nicht alltägliches Brot war und dahingehend war auch die Infrastruktur sehr sehr stark eingeschränkt in der Behandlung viele Themen in der internen Infrastruktur, da viele administrative Sachen einfach dazugekommen sind als Nebengeräusche.

21 Speaker 0 okay, also das beantwortet dann auch schon die Frage 4 mit: Wenn ja, welche Maßnahmen wurden gesetzt? Dann können wir mit der fünften Frage fortfahren. Und zwar: Haben diese Maßnahmen die Servicequalität im zufriedenstellenden Maß verbessert?

22 Speaker 1 Also die Maßnahmen haben sicherlich die Infrastruktur zufriedenstellend verbessert. Aber für die User nur zu einem gewissen Teil sage ich mal die Komplexität, dann die ganze Infrastruktur, das Handling des Arbeitsplatzes wurde um einiges erschwert. Also durch die Security Konzeptionen, die hier erstellt wurden und die umgesetzt wurden, hat sich zwar die Sensibilität ein bisschen verändert in die Richtung, dass auf Security um einiges mehr Wert gelegt wurde, allerdings auf Kosten der Usability, dass man jetzt versucht peu-a-peu abzufedern mit Schulungen und eben Zeit.

23 Speaker 0 Okay, dann wäre so eine Maßnahme wahrscheinlich für die Zukunft, dass die Dokumentationen intensiviert werden, damit die Enduser asynchron ohne Nachfrage die Usability erreichen können, wie es vor der Pandemie der Fall war.

24 Speaker 1 Genau da geht es dann auch speziell um Laptops, dann zum anderen mit Smartphones die ja auch immer mehr werden und immer intensiver genutzt werden. Und auch nützliche Gadgets in Richtung Firmenumgebung genutzt werden können und nicht

nur gesondert auf privat oder im Unternehmen, sondern dass hier das Gerät vereint werden kann für beide Welten.

25 Speaker 0 Dann fahren wir mit dem dritten Frageblock fort. Und zwar: Inwiefern helfen Monitoringlösungen, den laufenden Betrieb von IT Services und Infrastruktur zu unterstützen?

26 Speaker 1 Naja, Monitoringlösungen sind zum Großteil dafür da, die Administratoren in-House zu entlasten, indem die Administratoren hier nicht täglich Stunden oder Tage investieren müssen, um gewisse Services selber zu prüfen, sondern dass dies quasi automatisch passiert mit Gewissens Softwaretools wie SCOM, NAGIOS, PRTG und wie hier alle Hersteller heißen die Services, Server, Festplattengrößen, Dienste ganz einfach automatisiert prüfen, melden und reporten. Zudem bekomme ich durch diese Monitoringlösungen auch Reports. Wie oft habe ich Probleme auf dem einen System? Wie oft auf dem anderen System? Wo sind eventuell Punkte, wo man nachbessern kann auch Infrastruktur technisch um sich hieraus wieder Geld zu sparen. Also auch aus dem wirtschaftlichen Aspekte heraus gesehen würde ich in Mittel- bis Großunternehmen auf kein Monitoringsystem verzichten wollen.

27 Speaker 0 Okay, verstehe. Also ist es auch forciert worden, dass Monitoringlösungen bei bestehenden Kunden forciert worden sind, in der Betreuung als auch bei bestehenden Kunden wo noch kein Monitoringsystem im Einsatz war forciert worden ist, dass es implementiert wird.

28 Speaker 1 Ja, definitiv, die letzten zwei Jahre war hier nochmal ein großer Boost. Zwar nicht von den üblichen Herstellern wie SCOM, NAGIOS, PRTG, sondern haben eher die Monitoringdienste der Security Lizenzen, eine Microsoft Azure zurückgegriffen, um auch zum Beispiel die Clients ordentlich monitoren zu können. Egal von wo aus sich diese Clients melden, sei es Teleworking, sei es IT- intern eine Infrastruktur, damit eben auch die Security Seite geprüft werden kann, und tut sich auf diesem Client, welche Software wird installiert. Gibt es hier Angriffspotenziale? Dahingehend ist definitiv ein riesen Aufwand investiert worden, um diese Lücken zu stopfen. Eine große Hilfe der Administratoren eben in einem Angriffsfall zu wissen, wo ist dieser passiert und ja auch schnell zu schließen.

29 Speaker 0 Okay, verstehe hat es natürlich auch den proaktiven Wartungsaspekt bzw. Einsatzaspekt für Monitoring Lösungen sich daraus ergeben aus dem bestehenden Anforderungen das auch noch zu nutzen und den Schwung direkt mitzunehmen. .

30 Speaker 1: Korrekt

31 Speaker 0: Gibt es Fälle, in denen der Einsatz von Monitoringlösungen keinen Mehrwert bringt? Und wenn ja, welchen Grund hat dies?

32 Speaker 1 Ja, natürlich ist es auch immer wirtschaftlich zu sehen, welches und in welchem Ausmaß man ein Monitoringsystem implementiert. Für Kleinunternehmen oder für Einzelunternehmen, die im wesentlichen vielleicht aus zwei-drei Rechnern bestehen, einen Server laufen haben, keine kritische Infrastruktur am Leben erhalten müssen, muss ich natürlich auch die wirtschaftliche Frage stellen, ob eine Monitoringlösung um den Preis rechtfertigen würde eine gewisse Art von Umgebung zu Monitoren oder ob es der Administrator dann selber mit managen kann.

33 Speaker 0 Okay, versteh.

34 Speaker 1 das muss man eben dem wirtschaftlichen gegenüberstellen. Wie viel Zeit investiere ich als Administrator und wie viel kostet mich das Monitoringsystem? Daraus ergibt sich dann irgendwo ein Schwellwert wo man die Grenze ziehen kann oder sollte. Oder auch in welchem Umfang dann ein Monitoringsystem eingesetzt wird.

35 Speaker 0 Okay, ist es bei Ihnen auch schon der Fall gewesen, dass Sie oder bzw. das Ihr Unternehmen dort versucht die goldene Mitte zu finden, an Aufwand das Monitoringsystem im akzeptablen Maß einzusetzen und natürlich für den Kunden ein attraktives Paket zu schnüren an Kosten.

36 Speaker 1 Natürlich, Kunden die jetzt noch keine Monitoringsystem hatten und vielleicht auch noch etwas skeptisch waren wie nützlich, wie hilfreich so ein Monitoringsystem ist aufgrund von Unwissenheit, dort wurden teilweise auch zuerst mal

	Testsystem eingeführt, verschiedenen Monitoringsysteme ausprobiert, lizenzfreie, kostenpflichtige und daraus wurde dann quasi ein Paket geschnürt was dem Kunden am besten gefallen hat und dieses Paket dann auch implementiert und umgesetzt.
37	Speaker 0 Okay, sehr interessant. Dann sind wir schon bei den Abschlussfragen. Lieber Herr Experte, wie haben Sie das Interview empfunden?
38	Speaker 1 Das Interview war sehr angenehm. Sehr nettes Gesprächsklima.
39	Speaker 0 Haben Sie noch Anmerkungen zu den Fragen.
40	Speaker 1 Keine weiteren Anmerkungen zu den Fragen. Soweit alles sehr verständlich und gut ausformuliert.
41	Speaker 0 Haben Sie noch zusätzlichen Input zum Forschungsthema?
42	Speaker 1 Keinen zusätzlichen Input meinerseits zu den Forschungsthema notwendig.
43	Speaker 0 Könnten Sie eventuell noch einen kurzen Einblick geben, wie bei einem Kundensystem mit einer Monitoring Cloud-Lösungen die Architektur aufgebaut wurde bzw. wie wie es zu dem Einsatz zur Implementierung gekommen ist?
44	Speaker 1 Also im Speziellen, dass man quasi über Cloud jetzt Monitoringsysteme über on-premise monitored. Okay, da haben wir zum Beispiel Einsatzfälle, wo on-premise Monitoringsysteme laufen, diese Monitoringsysteme selber aber nicht gemonitored werden. Jetzt kann es natürlich zu einem Ausfall des Monitoringsystems kommen, wo uns niemand darauf hinweist, dass dies eben passiert ist. Dahingend sind zum Beispiel auch Cloudservices gewachsen, indem die uns dann über gewisse on-premise Störungen informieren können. Sprich wenn jetzt ein SCOM on-premise keine Daten mehr liefern kann aufgrund eines Fehlers in anderen Systemen, so kann uns immer noch ein Azure-Agent, der auf diesem Server läuft, die Info geben, dass der Server ein Problem hat und somit kann hier das Thema auch abgefedert werden. Dann wurde quasi über die Cloud eine zweistufige Lösung implementiert.
45	Speaker 0 Okay, sehr interessant wurde das mit einem Alerting oder umgesetzt? Oder wie wurde das umgesetzt?
46	Speaker 1 Das wurde mittels Alerting umgesetzt. Hier werden automatisch Mails generiert, die dann an den jeweiligen Administrator oder an den jeweiligen Consultant automatisch geliefert werden. Mit der Info, dass hier die on-premise Lösung Probleme macht.
47	Speaker 0 Okay, und hat das auch schon im laufenden Betrieb funktioniert? Funktioniert die Umsetzung, dass auch wirklich der Ausfall nicht bemerkt wurde und dann mit der Alertinglösung das ganze abgefangen wurde.
48	Speaker 1 Genau aufgrund von solchen Situationen ist es ja auch eigentlich entstanden. Wir hatten das in gewissen Bereichen schon beobachtet, dass wir hier teilweise mehrere Tage ohne Monitoringsystem unterwegs waren, das aber nicht zur Gänze aufgefallen ist, da man sich eben auf dem Monitoringsystem mit einem gewissen Teil verlasst oder verlässt. Und dahingehend hat man sich dann nach Alternativen umgesehen und da die Cloud momentan sowieso einen riesen Aufschwung erlebt, konnte man hier die Synergien perfekt nutzen und auch umsetzen.
49	Speaker 0 Ok, sehr interessant. Dann sind wir auch schon am Ende von unserem Interview. Ich bedanke mich, lieber Herr Experte und wünsche Ihnen alles Gute.
50	Speaker 1 Ich bedanke mich auch für Ihre Zeit. Herzlichen Dank!

ANHANG D - Experteninterview Person 3

1 Speaker 0 Hallo lieber Experte zu unserem Experten Interview heute zum Thema "Kennzahlen im Kontext des Infrastruktur Monitorings" Beginnen wir mit der Übersicht, also einleitend werden wir die Forschungsfrage einmal gemeinsam behandeln. Dann geht es zu den Einleitungsfragen. Danach folgen die Fragenblöcken 1 bis 3 und abschließend noch die Abschlussfrage Blöcke für eventuelle Ergänzungen oder Feedback. Die Forschungsfrage im Rahmen der Masterarbeit lautet "Wie haben sich mit vermehrten Einsatz von Teleworking Arbeitsplätzen in der Pandemie von Covid-19 die Anforderungen an Monitoring Kennzahlen für IT Operations verändert?" Beginnen wir mit den Einleitungsfragen. Wie viele Jahre haben Sie bereits Erfahrung mit Monitorenlösungen für IT-Infrastruktur sammeln können?

2 Speaker 1 Das Thema Monitoring begleitet mich eigentlich schon mein ganzes IT-Leben lang. Das sind über 20 Jahre; also 22-23 Jahre, immer mehr oder weniger je nach Position die ich begleitet habe. Aber es war immer Thema herauszufinden, was passiert ist oder vorab Fehler feststellen zu können, ist eine grundlegende Frage.

3 Speaker 0 Wie viele Jahre haben Sie bereits Erfahrung in der Betreuung Administration oder Projektmitarbeit von IT-Infrastruktur sammeln können?

4 Speaker 1 Ebenfalls über 20 Jahre.

5 Speaker 0 Bei wie vielen Kunden waren Sie in der Administration Betreuung oder Projektmitarbeit von IT-Infrastruktur beteiligt?

6 Speaker 1 Ich habe unzähligen Kunden, indem ich auch in anderen Systemenhäusern als Consultant gearbeitet habe, ich habe auch Posten begleitet, wo ich IT-Verantwortlicher gewesen bin oder in einem IT-Datacenter Team. Das heißt also natürlich, bei den Arbeitgebern wo ich im Team war ist es dieser eine Kunde gewesen, aber ich habe es jetzt nicht aufgezählt. Aber bei sämtlichen Kunden bei der Base-IT, wo ich im Einsatz war und auch bei den anderenauch Hunderte, vielleicht "Tausende".

7 Speaker 0 Dann beginnen wir mit dem ersten Frageblock. Und zwar: Hat sich im Rahmen der Pandemie von COVID-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?

8 Speaker 1 Ja, das hat sich merklich gesteigert. Das hat natürlich auch dazu geführt, dass man Infrastruktur mäßig überhaupt mal Telworking Arbeitsplätze ausbauen oder anbieten haben müssen. Ja, also man hat es schon gemerkt das März 2020 wie der erste Lockdown gekommen ist, sind einige Kunden gekommen und sind da praktisch drauf gekommen, dass ihre Teleworking Infrastruktur, die sie bis jetzt haben, die vielleicht von vereinzelten Leuten genutzt worden ist, einfach nicht ausreichend war für die Anzahl der User, die sie jetzt haben, da sie alle User nach Hause geschickt haben. Also abgesehen davon, dass sie überhaupt mal Notebooks anschaffen mussten, hat natürlich auch die Internetanbindung, Firewalls, wie viele VPN-Sessions gleichzeitig gehen überhaupt betrachtet werden müssen. Und dann ist man drauf gekommen, dass es nicht skaliert. Natürlich haben wir dann die Vorteile der Cloud genutzt und haben Infrastruktur in die Cloud verlagert oder eben Cloud Services wie von Microsoft Azure AD aufgebaut und so für die User angeboten, was natürlich auch ein anderes Monitoring bedingt. Also in der Cloud funktioniert auch das Monitoring anders als der andere Teil der Infrastruktur. Und das ist im Nachhinein erst nachgezogen werden, muss aber eigentlich nachgezogen werden.

9 Speaker 0 Also wie haben sich aufgrund des vermehrten Einsatzes von Teleworking Arbeitsplätzen die Anforderung an die IT-Infrastruktur geändert?

10 Speaker 1 Ja, die Hauptänderungen waren, dass einfach die Art, wie Services angeboten werden, sich ändern müssen hat, weil die User jetzt verteilt waren. Ich habe keinen Einfluss mehr drauf, wenn er bei mir im Unternehmen ist hat er einen Switchport und ist mit Gigabit angebunden. Alles wunderbar. Wenn er natürlich von zu Hause aus arbeitet, kommen andere Faktoren hinzu. Also ist schon mal rein von der Qualität des Services, wie gut ist die User Internetverbindung, wie gut ist die Internetverbindung des

Unternehmens, weil jetzt ist das der Flaschenhals. Alle kommen da herein und wie kann ich dies umgehen? Ist mein Service überhaupt performant erreichbar aus dem Internet? Ist er sicher erreichbar, also kann ich ihn absichern? Und das hat schon dazu geführt, dass die Topologie komplett geändert worden ist, dass wirklich Teile des Rechenzentrums in die Cloud ausgelagert worden sind. Damit sie näher beim User sind, damit die performant sind.

11 Speaker 0 Also kann man die dritte Frage beantworten. Also Wie haben sich diese Änderungen der Anforderungen an die Infrastruktur ausgewirkt? Dass das bestehende Konzept überdacht hat werden müssen und auf die geänderte Topologie dann hin optimiert hat werden müssen?

12 Speaker 1 Ja genau

13 Speaker 0 Dann können wir schon mit dem zweiten Block beginnen. Hat der vermehrte Einsatz von Teleworking Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Serviceumgebungen?

14 Speaker 1 Das kommt auf Design drauf an. Es hat Auswirkungen, jedoch negative? Das ist eine Frage die sich ein ITler eigentlich so nicht stellt. Das hat Auswirkungen. Und wenn sie negativ sind, dann müssen wir darauf reagieren und müssen es reparieren. Ich hab meine Infrastruktur auf gewisse Topologie hin designed skaliert sie vielleicht auch und dann ändern sich die Anforderungen plötzlich so radikal. Dann hat es sehr wohl negative Auswirkungen, weil ich wahrscheinlich nicht bedacht habe bei meinem Design Habe ich das vielleicht vorher in meinem Design schon berücksichtigt, weil ich vielleicht sagen wir mal 10% Teleworking Arbeitsplätze sowieso anbieten hab müssen. Dann geht es nur nur darum, wie gut habe ich das implementiert, dass es skalieren kann. Dann sind die Auswirkungen vielleicht nicht so negativ gewesen.

15 Speaker 0 Okay, damit haben wir glaube ich auch schon die Frage 2 gut beantwortet. Dann zur dritten Frage: Mussten aufgrund dieser wandelnden den Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Servicequalität beibehalten zu können? Und wenn ja, welche Maßnahmen würden gesetzt?

16 Speaker 1 Ja, also bei vielen Kunden sind wirklich Cloud Services praktisch aus dem Nichts implementiert worden. Es ist entweder der Service als IaaS in Cloud Rechenzentrum transportiert worden, weil dort einfach die Benutzer eine bessere Erreichbarkeit haben, als wie am Firmenstandort, bis hin zu, dass Remote Desktop Arbeitsplätze oder Web Published Applications in der Cloud angeboten wurden, die dann durchtunneln an Applikationen, die on-premise sind bzw. Teile des Services auch in der Cloud abgebildet worden sind. Konkrete Beispiele sind zum Beispiel Zeiterfassung. Die User sind zu Hause im Homeoffice, müssen trotzdem ein und ausstempeln. Es ist ein Webservice, der aus dem internen Netz erreichbar ist. Wie bringt man diesen sicher zu einen User ins Homeoffice? Da hilft z.B. der Azure Application Proxy. Das bedingt, dass ich nichts ins DMZ stellen muss, es ist eine gesicherte Verbindung mit einem Agent über https getunnelt. Ich kann Identifizierungen und Authentifizierungen aus dem Azure AD davorschalten mit Conditionale-Access-Policies und genauso MFA erzwingen. Also wirklich sicherstellen, dass nur User auf diese Applikation Zugriff haben, die diese auch brauchen und mit Authentifizierung extra abgesichert werden können. Also das ist jetzt nur ein Beispiel, wie gesagt, ein anderes ist Azure WVD. Wir reden jetzt viel von Microsoft Azure Cloud natürlich gibt sich andere Cloud-Anbieter welche es ähnlich anbieten. Dort habe ich aber keine Erfahrung. Wir bieten hauptsächlich die Produkte von Microsoft in der Cloud an, darum benenne ich die auch explizit. Azure WVD hat ja den selben Vorteil. Bevor ich das in der Cloud implementieren konnte, habe ich auch die on-premise hinter dem DMZ einen Remote Desktop Gateway gebraucht und vielleicht auch noch einen Loadbalancer davor schalten müssen, Authentifizierung mit VPN irgendwie mit ADFS Server MFA abbilden müssen. Das kann man sich alles sparen in der Cloud, das hat man sich per Mausklick konfiguriert und ind der vorhandenen Lizenz mitkonfiguriert. Man startet diesen Service und kann den Usern Windows 10 Desktops zur Verfügung stellen. Das ist sogar Windows 10 Desktop und kein Windows Server Betriebssystem. Denn in der Cloud gibt es Windows 10 multi-session-Betriebssysteme,

die nur in der Azure Cloud betrieben werden können. Und das Look-and-feel für den Benutzer ist wirklich eine Windows 10 Benutzeroberfläche.

17 Speaker 0 Okay, dann kommen wir auch schon zur fünften Frage vom zweiten Block: Haben diese Maßnahmen die Servicequalität und zufriedenstellende Maß verbessert?

18 Speaker 1 Meiner Meinung nach ja.

19 Speaker 0 Dann sind wir auch schon beim dritten Block mit der ersten Frage: Inwiefern helfen Monitoringlösungen, den laufenden Betrieb von IT Services und Infrastruktur zu unterstützen?

20 Speaker 1 Monitoringlösungen sind meines Erachtens zwingend notwendig, wenn ich redundante Konzepte betreibe. Denn wenn ich meine Services so die Designe das ein Teil ausfallen kann, ohne dass der Service an sich beeinträchtigt ist, muss ich es monitoren, sonst bekomme ich es ja nicht mit. Es ist eine schlechte Praxis, dass man die User monitoren lässt. Das ich sage man wartet bis jemand anruft, dass etwas nicht geht und dann schaue ich erst drauf. Monitoring sollen mir ja genau das ermöglichen. Einen Fehler zu erkennen, bevor oder oder einen Umstand zu erkennen, der zu Fehlern führen kann, bevor wirklich ein Ausfall passiert. Und dementsprechend gehört das Monitoring auch intelligent genug aufgesetzt.

21 Speaker 0 Also macht es auf jeden Fall Sinn, wenn man die Monitoringlösung nicht nur stiefmütterlich behandelt, sondern wirklich die Ressourcen auch bereitstellt und aufwendet, um das ganze System auch proaktiv zu warten, adaptieren und immer am aktuellsten Stand zu halten.

22 Speaker 1 Also wie gesagt, wenn ich von Redundanz rede, muss sich vom Monitoring automatisch reden. Wer also Monitoring wie schon im Namen steht, das heißt, ich muss proaktiv drauf schauen. Monitoring kann auch bedeuten, die tägliche Tasks eines IT Mitarbeiters sind es, auf die Systeme manuell zu schauen, ob alles läuft, ob alle Dienste laufen, ob die Festplatten nicht zulaufen. Das kann auch manuell passieren. Die Lösung die wir haben, ist ja ein Zusammenschluss von verschiedenen Diensten. Monitoring, Alerting, Eskalation, Ticketsystem, das alles spielt ineinander. Es kann ja mehrere Monitoring Lösungen betreiben, was oft auch Sinn macht. Es gibt Produkte, die dem Netzwerk Monitoring besser und andere, die sind eben im Windowsumfeld besser, wieder andere im Linuxumfeld. Ich denke die eierlegende Wollmilchsau gibt es da nicht wirklich und da muss es etwas trennen. Also wenn die vom Monitoring redet, dann rede ich von Systemen, wo ich proaktiv als Single Point of View sehe, wie es meinen Systemen geht. Ich kann ja trotzdem immer noch auf jedes Betriebssystem separat drauf schauen und mir die Ereignisanzeige durchklicken. Das ist auch eine Form von Monitoring, aber wir betreiben viele System Center Operations Manager, der sammelt mir eben von allen Agent-Managed Maschinen, die Ereignisseanzeigen zusammen und interpretiert die Nachrichten je nach dem Managementpack ich verwende. Das ist wirklich einfach um den Fehler schneller zu finden.

23 Speaker 0 Und gibt es Fälle, in denen der Einsatz von Monitoring Lösungen keinen Mehrwert bringt. Und wenn ja, welchen Grund hat dies?

24 Speaker 1 Ja, da gibt es derer einige. Also es bringt keinen Mehrwert, wenn wenn es keine Service Owner gibt. Manchmal bei Kunden sehe ich es, dass wenn das Monitoring Systemfehler meldet, dass auch die Administratoren des Monitoring System für die Behebung verantwortlich sind. Es hat meiner meinung nach keinen Sinn, weil für was habe ich Spezialisten im Datenbank, Serverumfeld oder sonst woher, wenn dann der, der das Monitoring System betreibt eine Datenbank Server reparieren muss. Also es müssen Services definiert werden und Serviceverantwortliche. Diese Serviceverantwortlichen haben die Aufgabe das Monitoring zu gestalten mit dem Monitoringteam, also der muss zum Monitoring Team gehen und sagen: von meinem Service ist wichtig, dieser Webserver, dieser Datenbank Server, das gehört zusammen, diese Dienste müssen laufen. Es gibt Services, die bedingen eine gewisse CPU Last. Da kann es sogar ein Fehler sein, wenn die CPU Last zu wenig ist. Vielleicht will er dann darüber informiert werden. Vielleicht soll beim Monitor einen Alarm generiert werden, wenn die CPU Last zu gering ist und nicht nur wenn sie zu hoch ist, weil das auch ein

Fehlverhalten implizieren kann. Und diese Fragen die gehören gemeinsam erarbeitet und dann das Monitoring System dementsprechend konfiguriert. Wenn ich das nicht so habe, so geht es um einen Mehrwert, dann bringt es mir wirklich einen Wert. Der zweite Grund war ein Monitoring System keinen Mehrwert bringt ist, wenn die Kosten des Monitoring System oder des Betriebs des Monitoring Systems, die des zu überwachenden Dienstes überschreitet. Also in großen Umgebungen vom System Center Operations Manager, der ja nicht geschenkt, dieser hat ja Lizenzkosten pro Agent. Aber ich muss auch noch eine separate Hardware Infrastruktur betreiben, die redundant und Ausfallsicher ist, die dementsprechend dann natürlich auch im Lifecycle der Hardware erneuert werden muss. Und ich brauche natürlich Manpower. Es müssen, um die Redundanz auch wieder gerecht zu werden, mindestens zwei Personen zu 50 prozent oder 30 prozent sich um das Monitoring System annehmen und kümmern. Die dann diese Tasks, wenn ein neuer Service bereitgestellt wird in der IT des Unternehmens das dazugehörige Monitoring machen zu können. Natürlich kann ich externe Dienstleister für diese Aufgaben dazu kaufen, aber die sind auch nicht kostenlos. Also wenn die Kosten des Monitorings dem Benefit des Systems das zum Monitoren übersteigt, dann bringt es nicht wirklich was.

25 Speaker 0 Da hätte ich vielleicht noch eine Zusatzfrage: Ist es auch bei Kunden so empfangen worden, die die Message dahinter, dass der Mehrwert doch die Kosten übersteigen kann und wird, wenn das sinnvoll implementiert worden ist?

26 Speaker 1 Natürlich haben wir zum Beispiel, greifen wir wieder zum System Center Operations Manager zurück, ein Sizing Excel Sheet, wo wir die zu erfassenden Systeme eintragen und dann schauen, was kommt raus und dann kommt heraus, wie eine Maschine mit 8 Kernen und 256gb RAM. Wir brauchen Datenbank Server, der in der-und-der Größe dimensioniert ist. Dann wissen die meisten Kunden dann sowieso schon: Ja, das will ich bereitstellen oder das will ich nicht bereitstellen. Die wissen sehr wohl, was das bei ihnen in Unternehmen kostet. Selbstverständlich gibt es dann oft Diskussionen und wenn wir dann weniger Assets monitoren etc. Natürlich kann man dann nur die hoch kritischen Maschinen monitoren und dann könnte es eben von der Leistung günstiger werden. Aber oft wächst dann das Monitoring System oft nicht mit, mit der Infrastruktur. Irgendwann ist dann der Punkt erreicht, wo wir natürlich dann empfehlen: Jetzt ist es aber wirklich an der Zeit eigene Hardware dafür anzuschaffen. Oft kommt man rein und sagt: Wir wollen ein mal irgend ein Monitoring. Was kann das? Dann setzt man ein Proof-of-Concept auf oder designed eine Monitoring Umgebung für eine Handvoll Systeme mit geringeren Ressourcen, einfach nur um den Kunden einführen: WIll er das überhaupt haben? Das muss man dann eben mit skalieren. Aber wenn mehrere Services überwacht werden, muss ich natürlich auch den Mehrwert des Service zusammenzählen, dann sieht es wieder anders aus.

27 Speaker 0 Hat sich dann im Zuge der Pandemie und der Umstellung von der Serviceanbietung auch der Bedarf Kundenseitig forciert für mehr Ressourcen, mehr Investitionen für Monitoring Systeme?

28 Speaker 1 Ja, aber seltsamerweise nicht klassisch unbedingt die Infrastruktur, da hat es sich eher gewandelt, denn in der Cloud ist es anders zu monitoren mit anderen Produkten teilweise integriert oder nicht. Dann kommt man einen Mix aus 2 Monitoring Systemen, die man dann vielleicht versucht sie zu verheiraten.von dem was wir jetzt ja immer geredet haben war Infrastruktur Monitoring, was auch natürlich die selbe Technik für Security Monitoring ist. Also klassisch, ich muss Logs irgendwo sammeln und irgendwo auswerten und ein schönes Dashboard zur Verfügung stellen. Es sie dann eher dorthin verlagert. Die User haben sich verteilt. Ich will wissen wer meldet sich wann von wo aus, mit welcher Stärke der Identifikation und der Authentifikation. Dann sind eher die Security Produkte auf diese Logs drauf gesetzt worden und nicht so sehr die die Infrastruktur. Es fehlt ja in der Cloud einiges weg an Infrastruktur welche ich monitoren muss. Aber dafür sind andere Punkte schwieriger zu Monitoren. Also wenn ich in Plattform-as-a-Service denke, ich habe das Betriebssystem nicht mehr in Verwaltung, wo ich einen Agenten installieren kann. Da brauche ich andere

	Möglichkeiten einen Webservice zu monitoren, die aber meistens von den Cloudanbietern zur Verfügung gestellt werden.
29	Speaker 0 Okay, wahrscheinlich in Form von APIs, die dann eifnach abzufragen sind?
30	Speaker 1 Bei Azure heißen diese Insights die dann im Log Analytics Workspace gesammelt werden, wo man dann Dashboards daraus generieren kann und Availability und die Performance, wo man natürlich auch Vorfälle ganz anders reagieren kann. Der Vorteil der Cloud ist es, dass ich nur das bezahle, was ich auch nutze. Das heißt, es kommen dann einfach so Fragen auf wie: meinem Webserver will nur Ressourcen geben, wenn er sie wirklich braucht. Und wenn er sie nicht mehr braucht und sollen sie wieder weggenommen werden. Dann brauche ich sie auch nicht weiter bezahlen. Also so zu skalieren mit Scale-Sets dass bei vielen Zugriffe auf meiner Homepage Service zusätzlich Ressourcen auf und ab dreht. Und das zu automatisieren, dafür hat man dann Werkzeuge in der Cloud. Klassisch wenn ich Infrastruktur on-premise betreibe, habe ich sowieso schon bezahlt ist es egal wenn diese durchlaufen. Man muss es irgendwo im Vorfeld bezahlen. Aber diese Frage stellt sich in der Cloud schon seit Beginn. Dafür gibt es auch Techniken seit Beginn der Cloud , denn für diese Anwendung ist es eigentlich entwickelt worden.
31	Speaker 0 Ja okay, dann sind ja jetzt auch schon vor dem Abschluss Fragen: Wie Haben Sie das Interview empfunden?
32	Speaker 1 Sehr angenehm Danke.
33	Speaker 0 Haben Sie noch Anmerkungen zu den Fragen?
34	Speaker 1 Na sehr gut, also ich hoffe, es sind die Fragen, die du brauchst in deiner Masterarbeit. Mir wären keine zusätzlichen eingefallen.
35	Speaker 0 Haben Sie noch zusätzlichen Input zum Forschungsthema?
36	Speaker 1 Nein, eher auf Hinblick zur Pandemie und Monitoring Kennzahlen. Die Hauptveränderung ist einfach, dass das Überwachen nicht mehr so auf den Service selbst fokussiert, sondern mit Differenzierung auf den einzelnen User, denn wenn sie on-premise läuft und alle greifen on-premise darauf zu, kann ich davon ausgehen, dass er auch performant ist. Wenn er jetzt irgendwo läuft und die User irgendwo sitzen, dann läuft der Service, es heißt aber nicht, dass es für jeden User performant ist. Das ist in ganz großen Umgebung, wo ich dann vielleicht darüber rede, dass es weltweit zugänglich sein soll. Gerade wenn es auch vielleicht weltweit angeboten werden muss hat dieses Service ganz andere Kennzahlen. Das war aber auch schon vor der Pandemie schon so.
37	Speaker 0 okay, natürlich ändert sie die Anforderung komplett. Wie und von welchen Stellen die Informationen zusammenfließen sollen. Was beachtet werden soll. Was überhaupt wo angeboten wird an Ressourcen. Da verändert sich die ganze Konstellation und im Serviceangebot. Dann bedanke ich mich für die Zeit und für tolle und intensive Gespräch und beende nun die Aufnahme.

ANHANG E - Experteninterview Person 4

1 Speaker 0 Guten Tag Herr Experte und willkommen zu unserem Experten Interview zum Thema Kennzahlen im Kontext des Infrastruktur Monitorings. Beginnen wir mit der Übersicht. Also am Beginn werde ich Ihnen die Forschungsfrage vorstellen. Dann will ich mit den Einleitungsfragen beginnen. Dann folgen die Frage Blöcke 1 bis 3 und am Ende ist der Abschlussfrage Block, wo Sie Ihr Feedback einwerfen können. Nun zur Forschungsfrage Wie haben sich mit vermehrten Einsatz von Teleworking Arbeitsplätzen in der Pandemie von Covid-19 die Anforderungen an Monitoring Kennzahlen für IT-Operations verändert. Die Einleitungsfragen: Wie viele Jahre haben Sie bereits Erfahrungen mit Monitoren Lösungen für IT-Infrastruktur sammeln können?

2 Speaker 1 Also ich bin circa 15 Jahre gesamt in der IT unterwegs und habe natürlich immer wieder mit Monitoring Systemen zu tun. Ich bin kein direkter Betreuer von Monitoring Lösungen, aber es wird als Werkzeug, muss als Werkzeug genutzt werden.

3 Speaker 0 Wie viele Jahre haben Sie bereits Erfahrung in der Betreuung Administration oder Projektmitarbeiter von IT-Infrastruktur sammeln können?

4 Speaker 1 In der Administration und Betreuung und auch in der Projekt Mitarbeit eigentlich auch über alle 15 Jahre.

5 Speaker 0 Bei wie vielen Kunden waren Sie in der Administration, Betreuung oder Projektmitarbeiter von IT-Infrastruktur beteiligt?

6 Speaker 1 Zwischen 10 und 20.

7 Speaker 0 Und abschließend: Mit welchen Monitoren Lösungen konnten Sie bereits Erfahrungen sammeln?

8 Speaker 1 Ja, nachdem wir als Base-IT SCOM (System Center Operations Manager) im Einsatz haben, natürlich mit dem SCOM, auch eine weit verbreitete Monitoring Lösung, die ich selber schon implementiert und administriert habe ist der PRTG und auch NAGIOS auf Basis von Checkmk. Das ist ein Framework für Nagios.

9 Speaker 0 Dann beginnen wir mit dem ersten Fragebogen: Hat sich im Rahmen der Pandemie von COVID-19 der Einsatz von Teleworking Arbeitsplätzen merklich gesteigert?

10 Speaker 1 Deutlich, ja auf jeden Fall. Also ich kenne eigentlich keinen Kunden, der keine Teleworking Arbeitsplätze im Einsatz hat. Wobei es natürlich heute Home-Office heißt und nicht mehr Teleworking.

11 Speaker 0 Wie haben sich aufgrund des vermehrten Einsatzes von Teleworking die Anforderungen an die IT-Infrastruktur geändert?

12 Speaker 1 Das ist eine sehr umfangreiche Frage in Wirklichkeit und ist stark davon vom jeweiligen Kunden bzw. von der jeweiligen Firma abhängig. Für manche würde ich behaupten gar nicht und für manche würde ich behaupten um 180 Grad. Es kommt ganz darauf an, wo der Einsatz ist. Wir bemerken bei uns in der Gesamtstruktur, dass es auf jeden Fall vermehrt, wie soll ich sagen, vermehrte das Applikations Development und Infrastruktur Richtung Cloud geht, weil das einfach flexibler ist, weil die vom Internet aus erreichbar ist. Ich brauch nicht eigene Systeme ins Internet zu publizieren, was natürlich immer ein Risiko ist. Deswegen geht man vermehrt auf Cloud-Lösungen hin. Jetzt nicht nur im Bereich von Infrastruktur-as-a-Service, wir schieben einen Server in die Cloud, sondern tatsächlich auf Cloud-Lösungen. Und das merkt man auch bei den Herstellern. Die großen Hersteller haben auf jeden Fall alle schon irgendwie, ein Angebot in der Cloud mit z.B. SAP, VMWare, Microsoft natürlich, etc..

13 Speaker 0 Und dann die dritte Frage: Wie haben sich diese Änderungen der Anforderungen auf die Infrastruktur ausgewirkt?

14 Speaker 1 Ja, also von der Technik her ist es relativ gleichgeblieben, da ist nicht allzu viel Neues dazugekommen. Viele betreiben die Infrastruktur so wie sie es hatten. Viele tendieren allerdings eben wie auch erwähnt Richtung Cloud Systeme. Heißt es wird nicht mehr darauf geschaut, dass man ein System bei sich am Server installiert, sondern dass man irgendwas verwendet, was in der Cloud schon präsent ist. Also mit

Cloud bitte auch generell alle Internet Möglichkeiten gemeint, nicht nur eine bestimmte Cloud wie AWS oder Azure, sondern generell übers Internet zugängliche Applikationen.

15 Speaker 0 Dann wären wir auch schon beim zweiten Folge Block bei der ersten Frage hat der vermehrte Einsatz von Televoting Arbeitsplätzen negative Auswirkungen auf bestehende IT-Infrastruktur und Service Umgebungen?

16 Speaker 1 Ähm, zumindest was den Aspekt Sicherheit betrifft, auf jeden Fall. Es gibt die Schwierigkeit, dass man Clients, die nicht im eigenen Haus stehen oder nicht im LAN stehen, sondern irgendwo im WAN sind, mit VPN verbunden sind, deutlich schwerer zu servicieren sind. Anfangen tut es eigentlich bei Updates. Es ist schwieriger, die Clients in einer vernünftigen Zeit zu erwischen. Und zum Beispiel Installationen, die wichtig sind, raus zu pushen etc., weil die Clients nicht immer online sind ja, diese ganze Push Mechanismus ist auf jeden Fall deutlich schwerer, was wiederum dazu führt, dass man Clients Zugriff gewährt, die nicht den Security Einstellungen entsprechen, die über normalerweise Active Directory oder so verteilt werden, sondern halt ja keine oder schlechte Einstellungen haben. Und das ist natürlich ein negativer Auswirkungen auf Security und man merkt es auch, dass die Security Angriffe in der letzten Zeit seitdem mehr Teleworking Arbeitsplätze gibt, auch die Security Angriffe auf Clients vorallem gestiegen sind und auch auf Kleinbetriebe.

17 Speaker 0 Okay, also kann man zusammenfassend sagen Die Compliance ist bei verteilten Systemen wie es ein Teleworking Arbeitsplatz dann auch darstellt wesentlich schwerer einzuhalten und auch in Griff zu bekommen.

18 Speaker 1 Genau schwieriger zum Monitoring, schwieriger zu erreichen und deswegen auch schwieriger Fehler zu beheben.

19 Speaker 0 Okay, damit hätten wir auch schon die zweite Frage beantwortet. Dann kommen wir gleich zur Dritten. Mussten aufgrund dieser wandelnden Anforderungen an IT-Infrastruktur Maßnahmen gesetzt werden, um die geforderte Service Qualität beibehalten zu können?

20 Speaker 1 Ja, auf jeden Fall. Also über sämtliche Applikationen hinweg. Der einfachste Weg ist normalerweise immer eine VPN Verbindung, die stark genug ist und dies natürlich direkt abhängig von Internetleitung. Also zumindest da ist auf jeden Fall in den letzten Jahren einiges an an Finanzen investiert worden. Und ja, wenn die Möglichkeit nicht gegeben ist, den Service on-premise oder in der eigenen Infrastruktur darzustellen, dann muss man auf einen Cloud Service gehen. Ja, und da steigen natürlich die Anforderungen an allen Seiten, würde jetzt behaupten, also sowohl an die Infrastruktur selbst, also an die Technik selbst als auch finanziell als auch an uns Know how der Mitarbeiter. Es ist irgendwie eine neue Sparte der IT, die die Cloud, auch wenn vieles gleich ist und nur "fancy" oder schön aussieht.

21 Speaker 0 Okay, und wenn ja, welche Maßnahmen wurden gesetzt, könnten Sie da eventuell ein spezifisches Beispiel erzählen?

22 Speaker 1 Ähm, ja, kann ich. Wir haben einen Kunden bei uns, der hat CAD Workstations im Einsatz. Diese CAD Workstations sind erstens teuer, zweitens klobig sind große Geräte, die, die man ungern auch als Firma außer Haus gibt, weil wegen dem Risiko. Weiters ist auf dem Desktop und Laptops hat man früher immer Security ein bisschen unterschieden, von Laptops hatte man gewusst, sie sind unterwegs und hat dementsprechend Verschlüsselung Maßnahmen gesetzt oder remote cleaning, remote locking so wie man es mit Mobiltelefonen macht. Da gibt es aus Intune Maßnahmen. Das ist bei oder kann bei Fat-Clients großen nicht mobilen Clients schwieriger sein. Und jetzt gibt es einen Fall bei uns, bei einem unserer Kunden, wo die CAD Workstations direkt in die Cloud verschoben werden. Die Anwendung wird in der Cloud gehostet und muss weltweit erreichbar sein mit der gleichen Servicequalität. Was nicht immer ganz einfach ist, weil einige Faktoren dazukommen. Also erstens ist eine Virtualisierung dabei, zweitens ist es der Internetleitung dabei und es ist auch für die Mitarbeiter teilweise eine Anpassung, wie gearbeitet wird ja.

23 Speaker 0 Okay, in welcher Form wurde das umgesetzt? Wurden dort in der Cloud ähnliche oder gleiche Ressourcen dazu gebucht und dann die Applikation mit diesen Ressourcen angebunden?

24 Speaker 1 Ja, im Prinzip ja. Ähnliche oder gleiche Ressourcen? Jein. Es wird natürlich versucht dann bei sowas zu standardisieren. Also es hat nicht jeder Mitarbeiter seinen eigenen Client, weil es einfach kostenmäßig nicht attraktiv genug ist, sondern man versucht es über (Ressourcen-)Farmen zu lösen. RDS Farmen, die eine Grafikkarte beinhalten und konkret haben wir das mit der Azure VDI Lösung implementiert. Und es funktioniert prinzipiell ganz gut. Aber es gibt natürlich wie gesagt dadurch, dass es halt per Internet erreichbar ist und dann Latenz riesengroße Rolle spielt. Gibt es einige Schwierigkeiten, mit denen man sich beschäftigen muss, die manchmal auch gar nicht technisch zu lösen sind, weil man kann die Leitung einfach nicht kürzer machen wie sie ist, sondern eventuell organisatorisch das irgendwie anders machen muss.

25 Speaker 0 Okay, haben diese Maßnahmen die Servicequalität im zufriedenstellenden Maß verbessert?

26 Speaker 1 Ähm, bei dem konkreten Beispiel? Jein. Für manche der Kollegen . für manche der Mitarbeiter, ja, die können jetzt schneller arbeiten wie vorher. Manche Mitarbeiter, die sehr, sehr gute Geräte on-premise hatten, also die, die tatsächlich teure Maschinen im Einsatz hatten, für die hat sich die Situation teilweise sogar verschlechtert.

27 Speaker 0 Dann wären wir auch schon beim dritten Frage Block. Bei der ersten Frage: Inwiefern helfen Monitoring Lösungen, den laufenden Betrieb von IT Services und Infrastruktur zu unterstützen?

28 Speaker 1 Also eine Infrastruktur ohne Monitoring Lösung zu betreiben ist grob fahrlässig ist. Es gibt sehr sehr viele Dinge, die man heutzutage monitoren muss. Angefangen von der Auslastung über die Erreichbarkeit von Services über eventuelle Security Incidents etc. etc. Monitoring Lösungen helfen dabei. Ja, das ist eigentlich nicht gar nicht in Worte zu fassen, wie sehr Monitoring Lösungen helfen und deswegen gibt es auch jede Menge davon. Manche speziell eingesetzt für Netzwerk Themen, manche speziell eingesetzt wie eben der SCOM für Windows Systeme. Genau.

29 Speaker 0 Okay, dann werden wir auch schon bei der zweiten Frage vom dritten Block: Gibt es Fälle, in denen der Einsatz von Monitoren Lösungen keinen Mehrwert bringt und wenn ja, welchen Grund hat dies

30 Speaker 1 in einem normalen Office Betrieb sage ich jetzt mal oder auch Produktionsbetrieb würde mir jetzt kein Grund einfallen, dass eine Monitoring Lösung keinen Mehrwert bringt. Ganz im Gegenteil, Monitoring Lösungen können einem Administrator helfen schnell zu bemerken, ob sich in seinem System irgendetwas tut, ob irgendwo etwas schief liegt etc. kann die Auslastung messen von meinem System kann darauf reagieren. Ich kann auf Statistiken zurückgreifen, um meine Systeme zu planen. Ohne Monitoring Lösung ist glaube ich heutzutage Administration nicht möglich.

31 Speaker 0 Okay, dann hätte ich vielleicht noch eine extra Frage, hat sich die Verwendung bzw. auch der Bedarf nach Monitoren Lösungen in den Betrieben mit den Umstellungen, die die Pandemie nach sich gezogen hat. Hat sich das ganze intensiviert und ist kundenseitig dort auch der Bedarf forciert worden?

32 Speaker 1 Auf jeden Fall. Monitoring Lösungen müssen mittlerweile nicht nur wissen, ob ein Service lebt oder nicht, sondern auch meist die Performance von dem Service messen. Ja, ich fange nochmal von vorne an. Also die müssen nicht nur wissen, ob der Service erreichbar ist, sondern müssen auch die Performance messen von dem Service nicht nur im Hinblick auf Server, sondern auch im Hinblick auf einzelne Applikationen Web Anwendungen zum Beispiel. Darüber hinaus teilweise sogar auf Clients. Das kann man nicht so oft vor, wird aber auch schon. Und natürlich, nachdem jetzt seine ganz neue IT-Branche entstanden ist in den letzten 10 Jahren, also diese Cloud muss auch die Cloud in irgendeiner Art und Weise gemonitored werden. Dadurch erhöhen sich natürlich enorm die Anforderungen an Monitoring Lösungen. Wie vorher erwähnt ist Security natürlich auch ein großer Faktor. Deswegen schaut man auch, dass diese Monitoring Lösungen nicht nur dieses Legacy Monitoring "funktioniert mein Zeug"

	machen können, sondern auch erkennen können, ob es denn ja einen Angriff gibt, ob irgendwo eine Securitylücke entstanden ist.
33	Speaker 0 Könnten Sie noch eventuell darlegen, inwiefern sich der Bedarf bei den Kunden geändert hat bzw. forciert hat? Sind die Kunden da gekommen und haben beispielsweise gesagt Okay, wir wollen jetzt vermehrt unsere Monitoring Lösungen für die Cloud noch zusätzlich ausbauen, im Hinblick eventuell zu Microsoft Azure?
34	Speaker 1 So könnte man es formulieren, wobei die Kunden normalerweise ja einen anderen Wortlaut verwenden. Es gibt selten Kunden, die sagen mein SCOM muss das und das Mitbringen, sondern die Frage kommt eher: Wie können wir die Maschinen dort auch mit monitoren? Wie können wir frühzeitig erkennen, ob es Security Lücken gibt? Wie können wir unsere Infrastruktur planen für die nächsten drei Jahre? Woher wissen wir, wie hoch das Wachstum auf Festplatten ist? Die Fragen kommen eher nicht so direkt zum Monitoring System, sondern ergeben sich daraus.
35	Speaker 0 Okay, also ergeben sich aus dem Kunden Bedarf und dann wird die Lösung dahingehend technisch zugeschnitten.
36	Speaker 1 Ganz genau
37	Speaker 0 Ok. Dann wären wir auch schon beim Abschlussfrage Block. Wie haben Sie das Interview empfunden?
38	Speaker 1 Sehr angenehm.
39	Speaker 0 Danke! Haben Sie noch Anmerkungen zu den Fragen?
40	Speaker 1 Nicht direkt.
41	Speaker 0 Haben Sie noch zusätzlichen Input zum Forschungsthema?
42	Speaker 1 Nein.
43	Speaker 0 Okay, dann bedanke ich mich für das tolle Interview und wünsche Ihnen noch alles Gute.
44	Speaker 1 Sehr gerne, danke ebenfalls.

ANHANG F - Paraphrasen und Kodierungen

Paraphrasen	***Codes***
9 Jahre Erfahrung mit Monitoringlösungen	Informationen über Experten
11 Jahre Berufserfahrung	Informationen über Experten
Erfahrung bei drei Umgebungen plus Erfahrungsaustausch mit Kollegen	Informationen über Experten
Erfahrung mit Nagios, WürthPhoenix NetEye, PRTG, Zabbix, upRobot, Splunk, Elasticsearch	Informationen über Experten
mindestens 6 Jahre Erfahrung mit Monitoringlösungen	Informationen über Experten
10 Jahre Erfahrung mit IT-Infrastruktur	Informationen über Experten
Erfahrung bei 30-40 Kundensystemen	Informationen über Experten
Erfahrung mit SCOM, Nagio, PRTG	Informationen über Experten
22-23 Jahre Erfahrung mit Monitoring	Informationen über Experten
über 20 Jahre Berufserfahrung	Informationen über Experten
Erfahrung bei mehr als 100 IT-Systemen	Informationen über Experten
15 Jahre Erfahrung mit Monitoringsystemen	Informationen über Experten
15 Jahre Berufserfahrung	Informationen über Experten
Erfahrung bei 10- 20 unterschiedlichen Umgebungen	Informationen über Experten
Erfahrung beim Monitoring mit SCOM, PRTG, NAGIOS mit checkmk	Informationen über Experten
Sofern es die Rolle erlaubt hat sich Teleworking merklich gesteigert	Einsatz von Teleworking
Es haben sich Anforderungen an Netzwerkinfrastruktur, Teleworkingclients, VPN Konfigurationen geändert	Auswirkungen auf Infrastruktur
Maßnahme wie Awareness-Schulungen für Anwender und IT-Betrieb eingesetzt	Maßnahmen zur Einhaltung der IT-Servicequalität
Anforderung an Anbindung gestiegen weil Trafficaufkommen sich ändert	Auswirkungen auf Infrastruktur
Maßnahme: Teleworking Regelung mit Fokus auf Security. Mehr Aufkommen von Cyberangriffen	Maßnahmen zur Einhaltung der IT-Servicequalität
positive Auswirkungen auf Infrastruktur, weil Unternehmen Wichtigkeit der Infrastruktur wahrnehmen und Maßnahmen zur Absicherung einleiten.	Auswirkungen auf Infrastruktur
User haben erhöhte Servicequalität besserer Verfügbarkeit, mehr Flexibilität und Sicherheit, kaum Einschränkungen	Einsatz von Teleworking, Auswirkungen auf Infrastruktur
Negative Auswirkungen bei schlechter Vorbereitung; Services können ausfallen, Verfügbarkeit eingeschränkt sein.	Auswirkungen auf Infrastruktur
Security und Clientmanagement bei manchen Unternehmen und Folgen nicht bewusst; Geringes Bewusstsein und keine Maßnahmen zur Absicherung haben großes Sicherheitsisiko	Auswirkungen auf Infrastruktur, Änderung in IT-Serviceerbringung
Trotz Teleworking bereits im Einsatz waren Optimierungen nötig.	Auswirkungen auf Infrastruktur
Maßnahmen zur Clientverwaltung, Netzwerksicherheit, Userschulung, Unterweisungen, Authentifizierung mit MFA	Maßnahmen zur Einhaltung der IT-Servicequalität

Servicequalität und Security konnte im zufriedenstellenden Maß verbessert werden;	Maßnahmen zur Einhaltung der IT-Servicequalität
Maßnahmen haben Servicequalität und Mitarbeiterproduktivität gefördert	Maßnahmen zur Einhaltung der IT-Servicequalität
Monitoring ist essentiell für IT-Operations; Helfen Überblick zu erhalten sowie Probleme, Fehler und Stillstände schneller zu lösen	Einsatz von Monitoring(lösungen)
Monitoring hilft proaktiv statt Reaktiv zu Handeln; Unterstützt bei Anforderung von hoher Verfügbarkeit von Services	Einsatz von Monitoring(lösungen)
Monitoring bringt keinen Mehrwert wenn nicht aktiv gepflegt, damit gearbeitet und darauf reagiert wird.	Einsatz von Monitoring(lösungen)
Bewusstsein für IT-Infrastruktur als Ruckgrat der Unternehmen fehlt noch; schlechte Absicherung führt zu Sicherheitsrisiken	Auswirkungen auf Infrastruktur
Mehrschichtigen Monitoring im Einsatz um Serviceerreichbarkeit von intern und extern zu gewährleisten zu können	Einsatz von Monitoring(lösungen)
Zentrales Dashboard hilft bei Übersicht und Handhabung des Monitorings	Einsatz von Monitoring(lösungen)
Logging als Teil des Monitorings hilft Compliance zu gewährleisten (Nachverfolgbarkeit)	Einsatz von Monitoring(lösungen)
Ressourcenaufwand für Implementierung und Betreuung des Monitorings erforderte vier Personen zumindest teilzeit	Einsatz von Monitoring(lösungen)
Teleworking merklich gesteigert seit Pandemie	Einsatz von Teleworking
Anforderungen haben sich bei Infrastruktur und Securitykonzepte verändert	Einsatz von Teleworking, Auswirkungen auf Infrastruktur
Monitoringkonzept musste adapiert und ausgebaut werden. Security und Clientmonitoring besonderer Stellenwert aufgrund der geänderten Anforderungen.	Auswirkungen auf Infrastruktur, Einsatz von Monitoring(lösungen)
Altlasten wurden aufgrund der negativen Auswirkungen aufgerollt und nachgebessert. Kritische Infrastrukturthemen wurden angepasst, haben zu verbesserungen geführt	Auswirkungen auf Infrastruktur
Sicherheitskritische Themen führten zu intensiven Monitoring von Teleworking Clients. Authentifizierungsmethoden und Fernzugriff wurden angepasst	Einsatz von Monitoring(lösungen), Monitoringkennzahlen
Infrastruktur wurde vereinheitlicht im Zuge von Neuanschaffungen	Auswirkungen auf Infrastruktur
Neue Infrastrukur musste in Monitoring eingebunden werden; wurde mit Vereinheitlichung vereinfacht.	Auswirkungen auf Infrastruktur, Einsatz von Monitoring(lösungen)
Schulungsmaßnahmen, um Servicequalität beibehalten zu können. Fernzugriff große Umstellung	Maßnahmen zur Einhaltung der IT-Servicequalität
Maßnahmen brachten zufriedenstellende Verbesserung	Maßnahmen zur Einhaltung der IT-Servicequalität
Security Maßnahmen haben Einfluss auf Usability von Services (Authentifizierung, Hürden); Bringt jedoch Sensibilität von Benutzer; Maßnahmen wie Schulungen helfen	Maßnahmen zur Einhaltung der IT-Servicequalität

Maßnahme wie ausführliche Dokumentation hilft Usability zu verbessern	Maßnahmen zur Einhaltung der IT-Servicequalität
Dokumentation für unterschiedliche Devices bei Servicenutzung sinnvoll	Maßnahmen zur Einhaltung der IT-Servicequalität
Monitoring hilft es Personal zu entlasten und Automatismen einzuführen für überwachung, alerting und reporting	Einsatz von Monitoring(lösungen)
Monitoring hilft proaktive Maßnahmen bei wiederkehrenden Problemen zu treffen. Monitoringsystem bei Unternehmen ab mittlerer Größe unverzichtbar.	Einsatz von Monitoring(lösungen)
Investitionen in Monitoring forciert.	Einsatz von Monitoring(lösungen)
Clientmonitoring forciert; besonders mit Fokus auf Security Themen und Softwareinventarisierung. Monitoring hilft bei Security Incident Problem zu erkennen und zu beheben.	Einsatz von Monitoring(lösungen), Monitoringkennzahlen
bei kleinen Infrastrukturen hat Monitoring wirtschaftlich wenig Sinn. Manuelles Monitoring praktikabler	Einsatz von Monitoring(lösungen)
Zu Beachten ist Grenze wann Umstellung auf automatisiertes Monitoring lohnenswert ist	Einsatz von Monitoring(lösungen)
Testsysteme helfen Nutzen von Monitoring zu verstehen wenn Implementierung geplant wird	
on-premise Monitoringlösungen werden mit Cloudlösungen verknüpft um Redundanzen zu schaffen	Einsatz von Monitoring(lösungen)
Cloudmonitoringlösungen helfen auf Problemen bei on-premise Lösung hinzuweisen	Einsatz von Monitoring(lösungen)
Redundanzen bei Monitoring wichtig	Einsatz von Monitoring(lösungen)
Teleworking merklich gesteigert. Bestehende IT-Infrastruktur nicht ausreichend. Skalierbarkeit fraglich. Kapazitäten fraglich. Cloud Modelle eingesetzt. Kombination aus on-premise und Cloud erfordern angepasstes Monitoring	Einsatz von Teleworking, Einsatz von Monitoring(lösungen), Monitoringkennzahlen
Serviceerbringung hat sich geändert. User verteilt, heterogene Infrastruktur, neue Faktoren bei Servicequalität. Bestehende Services über Internet performant und Sicher. Führte zu Topologieänderungen; Auslagerung in Cloud	Auswirkungen auf Infrastruktur, Änderung in IT-Serviceerbringung
Wenn Infrastruktur skalierbar und Teleworking unterstützt wurde, weniger Probleme bei Umstellung. Sonst Umstellung aufwendig da Infrastrukur umgebaut oder erweitert werden muss	Einsatz von Teleworking
Cloud Services wurden implementiert. Bereitstellung über Cloud simpler als on-premise bei skalierbaren Services. Für Enduser kaum unterschied in Benutzung.	Auswirkungen auf Infrastruktur, Änderung in IT-Serviceerbringung
Servicequalität ausreichend verbessert	Änderung in IT-Serviceerbringung
Monitoring essentiell um proaktiv handeln zu können	Einsatz von Monitoring(lösungen)
Redundante Konzepte erfordern Monitoring	Einsatz von Monitoring(lösungen)
Verschiedene Monitoringlösungen für Teilbereiche (Netzwerk, Security, Client, Server) und Spezialfelder sinnvoll	Einsatz von Monitoring(lösungen), Monitoringkennzahlen

Monitoringlösungen erleichtern als Single-point-of-view den Überblick zu behalten. Monitoringlösungen helfen bei Auswertung und weiterführend bei Problembehebung	Einsatz von Monitoring(lösungen), Monitoringkennzahlen
Serviceowner sehr wichtig. Aufgabentrennung bei Monitoring und Fehlerbehebung. Serviceowner und Servicedefinition essentiell	Einsatz von Monitoring(lösungen)
Enge zusammenarbeit zwischen Serviceowner und Monitoringteam. Architektur des Monitorings muss interdisziplinär erarbeitet werden um Mehrwert daraus zu generieren	Einsatz von Monitoring(lösungen), Monitoringkennzahlen
Kein Mehrwert wenn Kosten des Monitoring die Kosten die Kostenersparnis im Betrieb übersteigen. Monitoring erzeugt Kosten bei Personal, Hardware, Lizenzierung.	Einsatz von Monitoring(lösungen)
Kunden sehen bei Monitoringkonzeption bereits ob der Mehrwert den Ressourcenaufwand für die Implementierung gerechtfertigt	Einsatz von Monitoring(lösungen)
Proof-of-Concept hilft für Kunden eine Verständnis für die Wichtigkeit des Monitorings zu schaffen	Einsatz von Monitoring(lösungen)
Investitionen in Ressourcen für Monitoring gestiegen. Cloud und On-Premise Monitoring unterschiedlich zu monitoren.	Monitoringkennzahlen
Monitoring wurde Richtung Security für Infrastruktur und Services forciert.	Monitoringkennzahlen
Für Cloud Service Modelle ist Monitoring anders umzusetzen, meist mit Schnittstellen des Betreibers.	Monitoringkennzahlen
Cloud Service Modelle ermöglichen in Kombination mit Monitoring flexible Ressourcenbereitstellung. Ermöglicht Services bei sich ändernden Anforderungen automatisiert mitzuskalieren. On-Premise Infrastruktur erfordert Initialinvestition, Cloud nicht.	Einsatz von Monitoring(lösungen), Monitoringkennzahlen
Services werden Komplexer zu monitoren wenn Infrastruktur heterogener wird.	Monitoringkennzahlen
Seit Pandemie deutliche Steiergung von Teleworking Arbeitsplätzen bei Kundenumgebungen	Einsatz von Teleworking
Auswirkungen: Je nach bestehender Ausrichtung; gar nicht oder sehr stark. Wenn Kunden bereits gut vorbereitet waren für Teleworking waren wenige Anpassungen nötig	Auswirkungen auf Infrastruktur
Angebot an Cloud Produkten und Lösungen steigt deutlich.	Änderung in IT-Serviceerbringung
Eigene Applikationen öffentlich anzubieten birgt Security-Risiko; daher Tendenz eher Cloudlösung zu beanspruchen.	Maßnahmen zur Einhaltung der IT-Servicequalität
Umsetzung als Cloud Applikation direkt und nicht nur auf Basis von IaaS mit eigener Lösung bei Kunden. Lösungen dieser Art bei bekannten Herstellern bereits in Angebot	Auswirkungen auf Infrastruktur

Es wird sowohl bestehende Infrastruktur weiterbetrieben, als auch Cloud Lösungen in Anspruch genommen.	Auswirkungen auf Infrastruktur
Ja negative Auswirkungen gerade im Aspekt der Clientverwaltung und Security	Auswirkungen auf Infrastruktur
Clientverwaltung, Update Compliance, Software Compliance sind aufgrund der heterogenen Umgebungen schwerer geworden einzuhalten; Führt beim Zugriff in Firmennetzwerke zu Security Risiken	Auswirkungen auf Infrastruktur, Monitoringkennzahlen
Security Incidents in Form von Angriffen auf Clients haben sich in der Häufigkeit gesteigert	Auswirkungen auf Infrastruktur
Auswirkung: Teleworking erfordert umfangreicheres Monitoring; weil schwerer zu erreichen und schwerer Fehler zu beheben	Einsatz von Monitoring(lösungen)
Ja, Maßnahmen mussten gesetzt werden um Servicequalität beizubehalten	Änderung in IT-Serviceerbringung
Maßnahmen: VPN für Fernzugriff wenn möglich; Ansonsten intensivierung des Einsatzes von Cloudmodellen	Änderung in IT-Serviceerbringung
Einsatz von Cloud steigert Anforderungen an Technik, Ressourceneinsatz, Wissen der IT-Mitarbeiter	Änderung in IT-Serviceerbringung
Maßnahme: Auslagerung von Infrastruktur (der Clients) in Cloud, um eine standardisierte Lösung über alle Benutzer zu ermöglichen. Poolressourcen genutzt	Auswirkungen auf Infrastruktur, Maßnahmen zur Einhaltung der IT-Servicequalität
Auswirkungen: Neue Herausforderungen im Umgang mit zusätzlichen Zwischenebenen im Serviceangebot (im Bezug auf Latenz, Performance)	Änderung in IT-Serviceerbringung, Monitoringkennzahlen
Herausforderungen: Poolressourcen in Cloud haben Latenznachteile gegenüber on-premise Lösung.	Änderung in IT-Serviceerbringung, Monitoringkennzahlen
Servicequalität konnte nicht für alle Benutzer im Cloud Poolressourcen Beispiel zufriedenstellend gelöst werden, da davor teilweise on-premise Lösungen im Einsatz waren. Jedoch konnte für einige eine zufriedenstellene Lösung erreicht werden	Maßnahmen zur Einhaltung der IT-Servicequalität
Monitoringlösungen essentiell für IT-Betrieb	Einsatz von Monitoring(lösungen)
Kennzahlen für Monitoring wie Auslastung, Erreichbarkeit, Security Incidents sehr wichtig für Betrieb. Monitoringlösungen helfen dabei diese zu ermitteln.	Einsatz von Monitoring(lösungen)
Kein Grund ersichtlich wieso Monitoringlösungen keinen Mehrwert bringen	Einsatz von Monitoring(lösungen)
Monitoring ermöglicht Administration zu erleichtern; zeigt den Zustand der betrachteten Systeme, deren Performance und Probleme mittels Statistiken	Einsatz von Monitoring(lösungen)
Anforderungen an Monitoring ändern sich im Hinblick auf reinem IT-Infrastruktur Monitoring zu ganzheitlichen Servicemonitoring mit Integration von Cloud Modellen	Monitoringkennzahlen

Security Monitoring hat an Bedeutung enorm gewonnen	Monitoringkennzahlen
Kundenanforderungen haben sich im Hinblick zum Umfang und Fähigkeiten der Monitoringlösungen erweitert mit Blick auf zukünftige Infrastruktur Erweiterungen.	Einsatz von Monitoring(lösungen), Monitoringkennzahlen

ABKÜRZUNGSVERZEICHNIS

ITSM	IT-Service-Management
SLA	Service Level Agreement
OLA	Operational Level Agreement
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and related Technology
CSI	Continual Service Improvement
SLM	Service Level Management
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
IaaS	Infrastructure-as-a-Service
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
KPI	Key-Performance-Indikator
CMM	Capability Maturity Model
SEI	Softwareentwicklungsinstitut
PDCA Zyklus	Plan-Do-Act-Check Zyklus
COVID-19	Corona-Virus-Disease-2019 (Coronavirus-Krankheit-2019)

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Addy, R. (2007). *Effective IT service management. To ITIL and beyond!* Berlin, New York: Springer.

Axelos. (2019). *ITIL Foundation ITIL 4 edition. ITIL 4*. London: The Stationery Office Ltd.

Axelos. (2021). *What is IT service management?,* Axelos. Zugriff am 22.06.2021. Verfügbar unter: https://www.axelos.com/best-practice-solutions/itil/what-is-it-service-management

Bainey & Kenneth. (2016). *Integrated IT Performance Management*. Boca Raton: Taylor & Francis Group.

Beims, M. (2010). *IT-Service Management in der Praxis mit ITIL 3. Zielfindung, Methoden, Realisierung ; hier finden Sie, was Sie für die Foundation Zertifizierung über ITIL 3 wissen müssen* (2. Aufl.). München: Hanser.

Beims, M. (2012). *IT-Service Management mit ITIL. ITIL Edition 2011, ISO 20000:2011 und PRINCE2 in der Praxis*. München: Hanser.

Bogner, A., Littig, B. & Menz, W. (2014). *Interviews mit Experten*. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-19416-5

Bortz, J. & Döring, N. (2006). *Forschungsmethoden und Evaluation. Für Human- und Sozialwissenschaftler ; mit 87 Tabellen* (Springer-Lehrbuch Bachelor, Master, 4., überarb. Aufl., [Nachdr.]. Heidelberg: Springer-Medizin-Verl.

Brand, K. & Boonen, H. (2007). *IT Governance based on Cobit 4.1. A management guide* (ITSM library, 3. ed., 1. impr). Zaltbommel: Van Haren.

Buchta, D., Eul, M. & Schulte-Croonenberg, H. (2010). *Strategic IT-Management. Increase value, control performance, reduce costs* (3rd ed.). Wiesbaden: Gabler.

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-4. Notfallmanagement*. Zugriff am 05.04.2021. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik. (2020). *IT-Grundschutz-Kompendium*. Zugriff am 19.04.2020. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html;jsessionid=79365EA1E4779CB441B65FCD7F38E7B6.2_cid351

Cloud Security Alliance. (2011). *CSA Guide,* Cloud Security Alliance. Zugriff am 01.10.2021. Verfügbar unter: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqyPG2nK7zAhUWgf0HHdApCmIQFnoECAkQAQ&url=https%3A%2F%2Fdownloads.cloudsecurityalliance.org%2Fassets%2Fresearch%2Fsecurity-guidance%2Fcsaguide.v3.0.pdf&usg=AOvVaw3OEGdJjEzR7a4T762_jjLm

Dern, G. (2009). *Management von IT-Architekturen. Leitlinien für die Ausrichtung, Planung und Gestaltung von Informationssystemen* (Praxis, 3., durchges. Aufl.). Wiesbaden: Vieweg + Teubner.

Drucker & Peter. (1977). *People and Performance*. New York: Harper & Row.

Gabler Wirtschaftslexikon. (2018). *Key Performance Indicator (KPI)*. Zugriff am 01.07.2021. Verfügbar unter: https://wirtschaftslexikon.gabler.de/definition/key-performance-indicator-kpi-52670

Gläser, J. & Laudel, G. (2009). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* (3., überarb. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Goltsche, W. (2006). *Cobit kompakt und verständlich. Der Standard zur IT Governance - so gewinnen Sie Kontrolle über Ihre IT - so steuern Sie Ihre IT und erreichen Ihr Ziele* (Aus dem Bereich IT erfolgreich gestalten, 1. Aufl.). Wiesbaden: Vieweg.

Gregory, P. H. (2008). *IT disaster recovery planning for dummies*. Hoboken NJ: Wiley.

International Labour Office. (2020). *Teleworking during the COVID-19 pandemic and beyond : a practical guide*. Zugriff am 06.04.2021. Verfügbar unter: https://digitallibrary.un.org/record/3878775

Jones, D. (2011). *Creating Unified IT Monitoring and Management for Your Environment*. Realtime Publishers.

Kavis, M. J. (2014). *Architecting the Cloud*. New Jersey: Wiley.

Kersten, H. & Klett, G. (2017). *Business Continuity und IT-Notfallmanagement. Grundlagen, Methoden und Konzepte*. Wiesbaden: Springer Fachmedien Wiesbaden.

Klosterboer, L. (2008). *Implementing ITIL configuration management*. Upper Saddle River NJ: IBM Press/Pearson.

Martin Andenmatten. (2021). *IT Governance – die Voraussetzung für gelebte Service Management Kultur,* Disruptive agile Service Management | Vom Kennen zum Können zum Tun. Zugriff am 22.06.2021. Verfügbar unter: https://blog.itil.org/2011/03/it-governance-die-voraussetzung-fur-gelebte-service-management-kultur/

Mayring, P. (2015). *Qualitative Inhaltsanalyse. Grundlagen und Techniken*. Beltz.

Mell, P. M. & Grance, T. (2011). *The NIST definition of cloud computing.* Gaithersburg, MD: national Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Microsoft (Microsoft, Hrsg.). (2021). *Operations Manager key concepts*. Verfügbar unter: https://docs.microsoft.com/en-us/system-center/scom/key-concepts?view=sc-om-2019

Misoch, S. (2015). *Qualitative Interviews*. Berlin/München/Boston: De Gruyter Oldenbourg.

National Center for Immunization and Respiratory Diseases. (2020). *How COVID-19 Spreads,* CDC. Zugriff am 01.10.2021. Verfügbar unter: https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fcoronavirus%2F2019-ncov%2Fprepare%2Ftransmission.html

Olbrich, A. (2008). *ITIL kompakt und verständlich. Effizientes IT Service Management - den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen* (Studium, 4., erw. und verb. Aufl.). Wiesbaden: Vieweg+Teubner.

Pierre D. Landry. (2001). *The ISO 9000 Essentials. A Practical Handbook for Implementing the ISO 9000 Standards*. Toronto: Canadian Standards Association.

Raithel, J. (2008). *Quantitative Forschung. Ein Praxiskurs* (2., durchgesehene Auflage). Wiesbaden: VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH Wiesbaden.

REFA Group. (2021). *PDCA-Zyklus*. Zugriff am 02.07.2021. Verfügbar unter: https://refa.de/service/refa-lexikon/pdca-zyklus

Rensmann, J. H. & Gröpler, K. Dr. (1998). *Telearbeit. Ein praktischer Wegweiser*. Berlin Heidelberg: Springer Verlag Berlin Heidelberg.

Rudolph, S. (2009). *Servicebasierte Planung und Steuerung der IT-Infrastruktur im Mittelstand. Ein Modellansatz zur Struktur der IT-Leistungserbringung*. Dissertation. Technische Universität München, München.

Scheer, A.-W. (2006). *Corporate performance management. ARIS in practice*. New York NY: Springer.

Schiefer, H. & Schitterer, E. (2008). *Prozesse optimieren mit ITIL. Abläufe mittels Prozesslandkarte gestalten ; Compliance erreichen und Best Practices nutzen mit ISO 20000, BS 15000 & ISO 9000* (IT-Management und -Anwendungen, 2., überarb. Aufl.). Wiesbaden: Vieweg + Teubner.

Spörrer, S. (2014). *Business Continuity Management. ISO 22301 und weitere Normen im Rahmen der Informationstechnologie*. Wiesbaden: Springer Gabler.

TOPdesk. (2021). *Was ist ITIL?* Zugriff am 01.07.2021. Verfügbar unter: https://www.topdesk.com/de/glossar/was-ist-itil/