Nutzen- und hemmnisorientierte Evaluation einer Client Security Lösung am Beispiel von „HP Sure Admin“

Bachelorarbeit

vorgelegt am 10. Mai 2021

Fakultät Wirtschaft

Studiengang Wirtschaftsinformatik

Kurs WWI2018H

von

Peter Falterbaum

Betreuer in der Ausbildungsstätte:	DHBW Stuttgart:
HP Deutschland GmbH Holger Wenzel Senior Presales Technical Consultant	Prof. Dr. Sebastian Richter

Inhaltsverzeichnis

Abkürzungsverzeichnis IV

Abbildungsverzeichnis V

Tabellenverzeichnis VI

1 Einleitung 1
1.1 Problemstellung . . . 1
1.2 Zielsetzung . . . 2
1.3 Vorgehensweise . . . 3

2 Über Technologieanschaffung entscheiden 4
2.1 Technologieakzeptanz . . . 4
2.1.1 Akzeptanzbegriff . . . 5
2.1.2 Ziele der Akzeptanzforschung . . . 6
2.1.3 Zustandekommen von Akzeptanz . . . 6
2.1.4 Nutzen für die weitere Arbeit . . . 8
2.2 Technologieresistenz . . . 9
2.2.1 Resistenzbegriff . . . 9
2.2.2 Zustandekommen von Resistenz . . . 10
2.2.3 Konkrete Ursachen und Lösungsansätze der Resistenz . . . 12
2.2.4 Nutzen für die weitere Arbeit . . . 13
2.3 Kriterien der Enterprise Resource Planning (ERP)-Auswahl . . . 14
2.3.1 Wissenschaftlicher Stand . . . 14
2.3.2 Dimensionen der Auswahl . . . 15
2.3.3 Nutzen für die weitere Arbeit . . . 20

3 Methodik 21
3.1 Forschungsdesign . . . 21
3.2 Experteninterviews als Methode der empirischen Erhebung . . . 23
3.3 Qualitative Inhaltsanalyse als Methode der Datenauswertung . . . 29
3.4 Transkription . . . 30
3.5 Kodierleitfaden und Definitionen . . . 31

4 Auswahlkriterien von Client Security Lösungen 33
4.1 Funktionalität . . . 33
4.2 Interoperabilität . . . 36
4.3 Kosten . . . 38
4.4 Anbieter . . . 39
4.5 Benutzerfreundlichkeit . . . 41
4.6 Service und Support . . . 43
4.7 Modell der Auswahlkriterien der Client Security Lösungen . . . 44

5 Evaluation von HP Sure Admin 49
5.1 Zweck und Einsatz von HP Sure Admin . . . 49
5.2 Anwendung des Bewertungsmodells auf HP Sure Admin . . . 51

6 Resümee und kritische Betrachtung **55**

Anhang **57**

Literaturverzeichnis **148**

Abkürzungsverzeichnis

BIOS Basic Input/Output System

BSI Bundesamt für Sicherheit in der Informationstechnik

CMSL Client Management Script Library

ERP Enterprise Resource Planning

IS Informationssystem

IT Informationstechnologie

LAK Local Access Key

MIK Manageability Integration Kit

POC Proof of Concept

SCCM System Center Configuration Manager

SPM Secure Platform Management

TAM Technology Acceptance Model

TPB Theory of Planned Behavior

TRA Theory of Reasoned Action

UTAUT Unified Theory of Acceptance and Use of Technology

Abbildungsverzeichnis

1 Aufbau des Technology Acceptance Model nach Davis. 7
2 Resistenzmodell nach Lapointe. 11

3 Modell der Auswahlkategorien von Client Security Lösungen. 45

Tabellenverzeichnis

1 Überblick des Forschungsdesigns, der Zielsetzungen und der Aufbereitung in der schriftlichen Ausarbeitung. 22
2 Aufschlüsselung der Interviewpartner*innen, deren Positionen und die Dauer der Interviews. 28
3 Übersicht über die Unternehmen der befragten Personen. 29
4 Definition der Kategorien zur deduktiven Anwendung. 31

1 Einleitung

> *„The homo oeconomicus, who lives in the presence of and is possessed of certain goods and whose actions will result from his desire to obtain the greatest pleasure from the appropriation or "consumption" of the goods."*[1]
>
> – Vilfredo Pareto, *1912*

Dieses Zitat beschreibt den Zusammenhang von Wirtschaftsgütern jeder Art und den dazugehörigen Konsumenten. Es wird darauf abgezielt, dass Konsumenten einen Wohlgefallen an einem Gut finden müssen, um es zu akzeptieren und schlussendlich zu konsumieren. Ein klassisches Problem der verhaltensökonomischen Forschung, welches hierbei erläutert wird, ist die Erklärung und das Zustandekommen von Kaufentscheidungen. Vilfredo Pareto verwendete 1912 erstmals den idealbildlichen Begriff des „homo oeconomicus", welcher durch sein rationales Handeln ausschließlich auf den eigenen Nutzen bedacht ist und auf dieser Grundlage seine Entscheidungen trifft. Spätestens seit den von Kahnemann und Tversky geführten Untersuchungen wird diese Theorie auf empirischer Basis kritisiert.[2] Die Forschungen der Wissenschaftler kamen zu dem Ergebnis, dass das Verhalten von einzelnen Subjekten nicht ausschließlich in rationalen Ursachen begründet ist. Kahnemann und Tversky zeigen in ihren Untersuchungen unter anderem auf, wie verschiedene Verzerrungen der eigenen Wahrnehmung und die Berücksichtigung zu weniger Informationen das subjektive Verhalten prägen.

1.1 Problemstellung

In der wirtschaftlichen Praxis finden sich diese Theorien und insbesondere das Problem mangelnder Informationen wieder, sodass sich die Frage stellt, auf Grundlage welcher Faktoren potenzielle Käufer*innen ihre Entscheidung treffen und wodurch die Entscheidungen durch subjektive Wahrnehmungen beeinflusst werden.

Die vorliegende Arbeit greift dieses Problem an einer spezifischen Technologielösung des Herstellers HP auf. Das Unternehmen bietet seit circa einem Jahr die technische Sicherheitslösung *HP Sure Admin* für die eigenen Computerprodukte an und stellt eine geringe Nachfrage der Lösung fest. *HP Sure Admin* stellt den Nutzer*innen der Lösung eine neuartige Möglichkeit des Schutzes des Basic Input/Output System (BIOS)[3] von Clients[4] an. Die Anwendung erlaubt es, das BIOS mit Sicherheitszertifikaten zu verschlüsseln und über Fernmanagement oder die

[1] Pareto 1912, S. 466

[2] Vgl. Kahneman u. a. 1982

[3] Das BIOS ist die Firmware eines Computers und wird beim Starten desselben ausgelöst. Das BIOS wiederum löst den Start des Betriebssystem des Computers aus.

[4] Im Kontext dieser Arbeit beschreibt der Begriff *Client* im weiteren Sinne computergestützte Endgeräte. Im engeren, auf HP kontextualisierten Sinn bezeichnen Clients windowsbetriebene Endgeräte der Firma HP. Beispiele: Notebooks und Desktop-Computer (von HP).

Nutzung einer Smartphone-App das BIOS zu entschlüsseln. Damit bildet die Lösung einen alternativen Ansatz zum bewährten BIOS-Schutz, welcher die Zugangskontrolle zum BIOS mit einem Passwort ermöglicht. HP sieht in der Lösung eine technologische Innovation, welche den Kund*innen neue Funktionalitäten hinsichtlich der Computersicherheit ermöglichen soll. Aufgrund dieses unerwarteten Ausbleibens der Nachfrage drängt sich für das Unternehmen die Frage auf, welche Ursachen bisherige und neue Kunden davon abhalten, die Lösung zu verwenden und welche Faktoren zu einer Kaufentscheidung und Nutzung führen können.

Eine dedizierte Ursachenermittlung gestaltet sich problematisch, da bislang keine HP-Kunden existieren, die diese Lösung einsetzen und zur Befragung herangezogen werden könnten. Außerdem bildet BIOS-Security ein Nischenthema ab, welches durch den innovativen Ansatz dieser Thematik die Vergleichbarkeit zu anderen Lösungen erschwert.

1.2 Zielsetzung

Mit dieser Ausarbeitung wird die Evaluation von HP Sure Admin angestrebt, welche funktional die Verschlüsselung und Teile des Management des BIOS abdeckt. Bisher ist in der Praxis die Verschlüsselung des BIOS mittels Kennworts üblich. Der Einsatz von HP Sure Admin soll eine Verbesserung dieses Status Quo bezwecken und einen alternativen Ansatz des BIOS-Schutzes etablieren. Da neben der klassischen Passwort-Verschlüsselung des BIOS keine vergleichbaren Ansätze des BIOS-Schutz vorhanden sind, wird der Untersuchungsgegenstand dieser Forschungsarbeit zunächst abstrakter als Client Security Lösungen definiert, um allgemeingültigere Feststellungen bestehender Lösungen erforschen zu können. Client Security Lösungen bilden dem Verständnis des Autors nach eine Toolklasse ab, welche Software- und Hardwarekomponenten enthält, um die Sicherheit eines Endgerätes sicherzustellen. Als Endgeräte werden in der Betrachtung Notebooks und Desktop-PCs zusammengefasst, da eine Berücksichtigung jeglicher Endgeräte für den Rahmen dieser Arbeit zu unspezifisch wäre und die verschiedenen Klassen der Endgeräte sehr heterogene Eigenschaften haben, was eine sinnvolle Abstraktion deren Eigenschaften infrage stellt. Notebooks und Desktop-PCs hingegen sind zwei sehr ähnliche Klassen, was die Eigenschaften Betriebssystem, Hardware und (physische) Schnittstellen betrifft. Als Sicherheitslösung wird dabei jeder Mechanismus verstanden, der die unmittelbare Erhöhung der Sicherheit eines Endgerätes bezweckt. Beispielweise sind an dieser Stelle Sicherheitslösungen für die Bereiche Virenschutz und VPN-Lösungen als Schutz vor Datenabgriffen genannt. Es werden jedoch auch sehr hardwarenahe Lösungen, wie eine Festplattenverschlüsselung oder Wiederherstellungsverfahren als Teil dieser Toolklasse verstanden. Im weiteren Verlauf wird diese Toolklasse als Client Security Lösung bezeichnet werden.

Durch die bereits geschilderte Situation sollen im Rahmen dieser Forschungsarbeit Einflussfaktoren ermittelt werden, die den derzeitig geringfügigen Einsatz der HP Client Security Lösung ergründen.

Erstes Ziel ist die Erstellung eines Modells, in welchem Auswahlkriterien von Client Security Lösungen und deren Beziehung untereinander abgebildet werden. Als weiterführendes Ziel soll anhand des Modells eine Evaluation von Client Security Lösungen am Fallbeispiel von HP Sure Admin durchgeführt werden.

1.3 Vorgehensweise

In den theoretischen Grundlagen dieser Arbeit sollen tiefere Kenntnisse zu Akzeptanz- und Resistenzfaktoren entwickelt werden. Hierzu werden zwei verschiedene Modelle als Referenz der Thematik herangezogen und durchleuchtet. Die Akzeptanz- und Resistenzmodelle sollen dazu beitragen, ein fundiertes Verständnis möglicher Einflussfaktoren zu entwickeln.

Des Weiteren wird Literatur zu Enterprise Resource Planning (ERP)-Systemen verwendet. ERP-Systeme sind bereits etablierte Lösungen in Unternehmen, die als Vergleichsbasis in dieser Arbeit verwendet werden. Es gilt, Akzeptanzen und Resistenzen in Bezug auf diese Systemart zu identifizieren, die im folgenden Verlauf als mögliche Akzeptanzkriterien für Client Security Lösungen geprüft werden. Die ermittelten Akzeptanzkriterien von ERP-Systemen werden gemeinsam mit weiteren identifizierten Kriterien der vorangestellten Modelle, zur Erstellung eines Interviewleitfadens verwendet.

Durch den Mangel an Kunden, die bereits HP Sure Admin einsetzen, werden Bestandskunden von HP aus unterschiedlichen Branchen zu ihren Beweggründen beim allgemeinen Einsatz von HP-Produkten befragt. Dies erfolgt durch insgesamt neun Experteninterviews. Die entstehenden Aussagen werden nach der qualitativen Inhaltsanalyse nach Mayring deduktiv ausgewertet und gegen die verwendeten Akzeptanzkriterien geprüft.

Auf dieser Basis wird nachgehend ein Modell zu Akzeptanzkriterien von Client Security Lösungen erstellt. Dabei wird zusätzlich auf die Wechselwirkungen der einzelnen Faktoren untereinander eingegangen.

Als Ergebnis dieser Arbeit und als Beantwortung der Forschungsfrage sollen Auswahlkriterien der Client Security Lösungen festgehalten werden und deren Konstellation zueinander erläutert werden. Darüber hinaus soll außerdem mithilfe der erschlossenen Kriterien eine Evaluation am Fallbeispiel von HP Sure Admin erfolgen und die Frage beantworten, inwiefern diese spezifische Client Security Lösung die Auswahlkriterien von Client Security Lösungen erfüllt.

Die konkrete Forschungsfrage, die im Kontext dieser Arbeit beantwortet wird, lautet somit wie folgt:
Welche Nutzenpotenziale und Resistenzfaktoren stehen sich bei der Entscheidungsfindung von Kund*innen zum Einsatz einer Client Security Lösung gegenüber?

2 Über Technologieanschaffung entscheiden

Zielsetzung: Die nachfolgende Aufarbeitung des aktuellen Forschungsstands basiert auf grundlegender Literatur zu den Themen Technologieakzeptanz und -resistenz sowie der Erforschung von Kriterien der ERP-Auswahl und dient als Fundament, um Kategorien für die qualitativ-deduktive Inhaltsanalyse abzuleiten. Mithilfe der literarischen Untersuchung sollen bestehende Ansätze zur Erschließung der Forschungsfrage offengelegt werden.

Aufbau: Zunächst führt dieses Kapitel die Überlegungen des letzten Kapitels bezüglich der Auswertung der erhobenen Daten detaillierter fort und beschreibt sowohl das Vorgehen der Transkription als auch die Umsetzung der Inhaltsanalyse deduktiver Kategorienanwendung. Anschließend erfolgt die tatsächliche Auswertung, strukturiert in Unterkapiteln je herangetragene Kategorie. Die Feststellungen der einzelnen Kategorien werden im letzten Unterpunkt zusammengetragen und in einem Verständnismodell manifestiert.

2.1 Technologieakzeptanz

Die Theorien der Technologieakzeptanz untersuchen verhaltenswissenschaftlich Ursachen, Einstellungen und Verhalten von Individuen. Sie zielen darauf ab, Aussagen über die logischen Zusammenhänge treffen zu können und insbesondere das manifestierte Entstehen von Akzeptanzverhalten erklären zu können.[5] In der Literatur haben sich Technologieakzeptanzmodelle mit abstrahieren Aussagen über die Nutzung und Akzeptanz von Technologien etabliert. Die Modelle stellen einen Bezug zwischen den einflussnehmenden Ursachen und der resultierenden Akzeptanz einer Person her, durch welche die Nutzung einer Technologie abgeleitet werden kann.[6] Die Technologieakzeptanzmodelle zeigen folglich eine Systematik auf, mit welcher die Einführung von Technologien anhand der Akzeptanz der Individuen bewertet werden kann. Eine hohe individuelle Akzeptanz könnte beispielsweise als Indikator für eine erfolgreiche Technologieeinführung sprechen.[7] In der Literatur wird als Ursprung für den wissenschaftlichen Diskurs der Technologieakzeptanzmodelle weitläufig das Technology Acceptance Model (TAM) von Davis genannt.[8] Davis stellte TAM 1985 im Rahmen seiner Dissertationsschrift vor[9] und seitdem wurde das Modell, auch von Davis selbst, weiterentwickelt, sodass mittlerweile eine Vielzahl unterschiedlicher, auf TAM beruhender Modelle in der Literatur vorzufinden sind.[10] TAM ist mittlerweile in der Literatur derart verbreitet und adaptiert worden, dass die Entwicklung des Modells als selbstständiger Untersuchungsgegenstand erforscht

[5] Vgl. Davis 1985, S. 25 f.
[6] Vgl. Davis/Bagozzi/Warshaw 1989, S. 985
[7] Vgl. Davis/Bagozzi/Warshaw 1989, S. 987
[8] Vgl. Vogelsang/Steinhüser/Hoppe 2013, S. 1425
[9] Vgl. Davis 1985, S. 24 ff.
[10] Vgl. TAM2 (Vgl. Davis 1985, 135 ff.), TAM3 (Vgl. Davis 1985, 140 ff.) oder auch: Unified Theory of Acceptance and Use of Technology (UTAUT) (Vgl. Venkatesh/Morris u. a. 2003, S. 447)

wird.[11] Das Modell gilt als initialer Ansatz, um die Akzeptanz einer Person in Bezug auf Technologie und deren Einflussfaktoren zu beschreiben und zu erklären.[12]

Am Anfang dieses Kapitels werden die Ziele, welche mit der Entwicklung und den Erweiterungen des Modells einhergingen, vorgestellt, um festzuhalten, was das Modell bezwecken soll und um resultierende Anwendungsszenarien von TAM aufzuzeigen. Anschließend wird das ursprüngliche TAM nach Davis[13] in seiner Ausgestaltung, Logik und Aufbau beschrieben und erklärt. Der darauffolgende Abschnitt diskutiert auf TAM aufbauende Modelle hinsichtlich der Nützlichkeit für die Beantwortung der festgelegten Forschungsfrage. Abschließend wird im vierten Teil des Kapitels die Anwendbarkeit des Modells für diese Arbeit abgewogen und aufgezeigt, inwiefern TAM für die Beantwortung der Forschungsfrage einbezogen werden kann.

2.1.1 Akzeptanzbegriff

Das Konstrukt der Akzeptanz wird in diversen Themenbereichen eingesetzt, sodass eine Differenzierung des Begriffs je nach Kontext notwendig erscheint. Je nach Themenfeld zeigen folglich verschiedene Indikatoren die Existenz von Akzeptanz an.[14] In einem wirtschaftlichen Kontext wird Akzeptanz vor allem für die Einführung von neuartigen Produkten verwendet. Akzeptanz „bezeichnet die positive Annahmeentscheidung einer Innovation durch die Anwender“[15], wobei zwischen *Einstellungsakzeptanz* und *Handlungsakzeptanz* unterschieden werden kann.[16]

Das Konstrukt der **Einstellungsakzeptanz** unterstellt eine positive Korrelation zwischen Einstellung und Akzeptanz eines Einzelnen, sodass bei der Annahme einer positiven Einstellung eine positive Akzeptanz des Nutzenden erwartet werden kann.[17] Die Einstellung der Individuen lässt sich dabei auf emotionale und kognitive Faktoren zurückführen. Emotionale Faktoren drücken sich durch regelmäßige Gefühlszustände gegenüber der Innovation aus.[18] Kognitive Faktoren umfassen die Bilanzierung von Kosten und Nutzen der Innovation aus der individuellen subjektiven Perspektive.[19]

Die **Verhaltensakzeptanz** ist die beobachtbare Folge der Einstellungsakzeptanz und geht über die Einstellungsbildung hinaus.[20] Sie indiziert eine Akzeptanz durch das aktive Verhalten (beispielsweise die Nutzung oder Adaption einer Innovation) eines Individuums.[21]

[11] Lee/Kozar/Larsen 2003
[12] Vgl. Vogelsang/Steinhüser/Hoppe 2013, S. 1425
[13] Vgl. Davis 1985, S. 24 ff.
[14] Vgl. Kollmann 1998, S. 37 ff.
[15] Simon 2001, S. 87
[16] Vgl. Müller-Böling/Müller 1986, S. 23 ff.
[17] Vgl. Kollmann 1998, S. 52
[18] Vgl. Müller-Böling/Müller 1986, 25 f.
[19] Vgl. Simon 2001, S. 87
[20] Vgl. Kollmann 1998, S. 52
[21] Vgl. Simon 2001, S. 87

2.1.2 Ziele der Akzeptanzforschung

TAM entstand aus der Zielsetzung, Akzeptanz im organisationalen Kontext durch Untersuchungen besser verstehen und beschreiben zu können.[22] In der Praxis soll das Modell der Prognose und Beschreibung von Nutzerverhalten dienlich sein und ursächliche Determinanten definieren.[23] Initial wurde mit der Erstellung des Modells einerseits das Ziel, die Nutzerakzeptanz als Prozess zu verstehen und aus einer theoretischen Betrachtung zu erfassen, wie das Erstellen und Implementieren von Informationssystem (IS) verbessert werden kann, sodass eine Nutzerakzeptanz der Technologien die Folge ist.[24] Andererseits strebte Davis an, mithilfe des fertigen Modells die tatsächliche Akzeptanz von Nutzern testen und vorhersagen zu können.[25] TAM dient also dazu, kausale Verbindungen zwischen Einflussfaktoren und der Akzeptanz von IS herzustellen, um damit das Verhalten von Nutzer*innen erklären und prognostizieren zu können. Das Modell kann gemäß der Zielsetzung genutzt werden, um das Problem zu untersuchen und dabei herauszufinden, welche Faktoren dazu führen, dass Änderungen von Systemen und Technologien von einzelnen Nutzenden, die keinen Einfluss auf die Einführung hatten, akzeptiert werden.[26] TAM kann also für die Akzeptanzuntersuchung von Innovationen genutzt werden. Prinzipiell ist TAM jedoch für Vorhersagen anwendbar, solange den untersuchten Individuen die Technologie bisher unbekannt ist.

2.1.3 Zustandekommen von Akzeptanz

Das TAM von Davis beruht auf dem Modell der Theory of Reasoned Action (TRA) und der Theory of planned Behavior.[27] In TRA wird festgehalten, dass die Absicht eines Einzelnen, ein bestimmtes Verhalten durchzuführen, eine direkte Determinante für die tatsächliche Ausführung des Verhaltens ist.[28] Die Verhaltensabsicht hängt wiederum von den Faktoren *Subjektive Norm* und *Einstellung in Bezug auf das Verhalten* ab.[29] Ist der Gegenstand der Betrachtung die Akzeptanz, so stellt TRA die Akzeptanzeinstellung mit dem Akzeptanzverhalten in eine kausale Abhängigkeit. In TAM wird diese Abhängigkeit aufgenommen und auf den Gegenstand *Technologie* angewendet. TRA unterstellt dem Individuum keine Limitation in der Verhaltensausprägung, was aufgrund von individuellen Unterschieden bezüglich Zeit, Kompetenzen und Fremdbestimmtheit unrealistisch erscheint.[30] Infolgedessen wurde das Modell um die Komponente *Wahrgenommene Verhaltenskontrolle* („Perceived Behavioral Control“) zur Theory of Planned Behavior (TPB) erweitert.[31] Je höher die wahrgenommene Verhaltenskontrolle der In-

[22] Vgl. Davis 1985, S. 25 f.
[23] Vgl. Davis/Bagozzi/Warshaw 1989, S. 985
[24] Vgl. Davis 1985, S. 6 f.
[25] Vgl. Davis 1985, S. 7
[26] Vgl. King/He 2006, S. 740
[27] Vgl. Davis 1985, S. 15 ff.
[28] Vgl. Madden/Ellen/Ajzen 1992, S. 4 f.
[29] Vgl. Davis/Bagozzi/Warshaw 1989, S. 983 f.
[30] Vgl. Jungbauer 2014, S. 50 f.
[31] Vgl. Madden/Ellen/Ajzen 1992, S. 4

dividuen, beispielweise ausgelöst durch das Empfinden, mehr Ressourcen oder mehr Möglichkeiten zu haben, desto höher ist nach TPB die Verhaltensabsicht und das daraus resultierende, manifestierte Verhalten.[32]

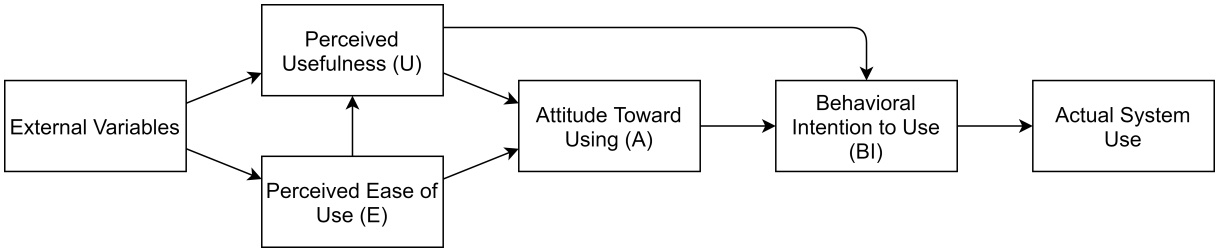

Abb. 1: Aufbau des Technology Acceptance Model nach Davis.[33]

Die Kernaussage von TAM ist, dass die individuelle Akzeptanz von Technologien von den zwei Determinanten *wahrgenommene Nützlichkeit* und *wahrgenommene Benutzerfreundlichkeit* abhängt.[34] Wie Abbildung 1 zeigt, ergibt sich aus diesen beiden Faktoren nacheinander die *Einstellung gegenüber der Nutzung*, die *Verhaltensabsichten* und die *tatsächliche Nutzung*. Die genannten Komponenten korrelieren dabei alle positiv in der genannten Reihenfolge, sodass eine hohe *wahrgenommene Nützlichkeit* und *wahrgenommene Benutzerfreundlichkeit* letztlich zu einer hohen *tatsächlichen Nutzung* führen.[35] Die *wahrgenommene Nützlichkeit* wird definiert als ein Grad dafür, wie hoch ein Individuum die Steigerung der eigenen Arbeitsleistung durch die Nutzung einer Technologie abschätzt.[36] Die *wahrgenommene Benutzerfreundlichkeit* hingegen wird definiert als Maß dafür, wie frei das nutzende Individuum von physikalischen und mentalen Anstrengungen bei der Nutzung der Technologie ist.[37]

Verschiedene Untersuchungen haben die logische Unterstellung von TAM mit quantitativen Studien statistisch überprüft und eine statistische Signifikanz der Beziehungen von wahrgenommener Benutzerfreundlichkeit, wahrgenommener Nützlichkeit und Nutzverhalten bestätigt.[38] Diese wissenschaftliche Bestätigung des aufgestellten Modells und der triviale Aufbau haben unter anderem zu einer hohen Verbreitung von TAM geführt. Das Modell eignet sich jedoch aufgrund der abstrakt beschriebenen Variablen nicht für ex ante Erklärungen, welche Prognosen erlauben würden. Daher ist der Anwendungsnutzen des Modells in dieser Weise beschränkt.

Der größte Vorteil von TAM ist die breite Anwendbarkeit des Modells aufgrund der abstrakten

[32] Vgl. Madden/Ellen/Ajzen 1992, S. 4
[33] Vgl. Davis 1989, S.319
[34] Die Variablen aus TAM werden verschieden ins Deutsche übersetzt. In dieser Arbeit wird ausschließlich die genannte Begrifflichkeit benutzt.
[35] Vgl. Davis/Bagozzi/Warshaw 1989, S. 985
[36] Vgl. Davis 1985, S. 26
[37] Vgl. Davis 1985, S. 25
[38] Vgl. Venkatesh/Davis 2000, S. 186

Variablen. Zugleich erschwert diese Generalität die spezifische Anwendung von TAM, welche Prognosen zulassen würden. Um diesem Kritikpunkt nachzukommen wurde das TAM in der Literatur verschiedentlich erweitert und spezifiziert.[39] In dieser Arbeit wird dieser Kritikpunkt jedoch in der Weise beachtet, dass neben der Akzeptanz die gegenteilig verortete Resistenz von Individuen berücksichtigt werden. Außerdem zeigten Untersuchungen, dass die wahrgenommene Benutzerfreundlichkeit im Allgemeinen einen relativ geringen und eher nicht signifikanten Einfluss auf die Akzeptanz einer Person hat.[40] Falls jedoch die tägliche Arbeit mit der Benutzung der Technologie einhergeht, konnte nachgewiesen werden, dass die wahrgenommene Benutzerfreundlichkeit einen hohen Einfluss auf die Akzeptanz hat.[41]
Der Untersuchungsgegenstand dieser Arbeit stellen Client Security Lösungen dar. Aufgrund der Tatsache, dass diese vor allen Dingen durch Administrator*innen in der täglichen Arbeitsroutine bedient werden, wird die Prämisse unterstellt, dass die wahrgenommene Benutzerfreundlichkeit einen Einfluss auf die Akzeptanz der Administrator*innen hat.

2.1.4 Nutzen für die weitere Arbeit

Zunächst bieten die dargestellten Thesen der Akzeptanzforschung einen Verständniszugang der Erforschung von Resistenzen in Abschnitt 2.2 an, welche mit einer ähnlichen Argumentation von Ursachen, Einstellungen und Verhalten argumentieren.

Außerdem bieten die aufgeführten Erkenntnisse der Akzeptanzforschung der vorliegenden Arbeit einen Argumentationsnarrativ an, welches das Verhalten und die Einstellungen von Individuen in Bezug zu bestimmten Ursachen setzt. Weiterführend streichen die Akzeptanzmodelle den Aspekt der subjektiven Wahrnehmung heraus, welcher in der qualitativen empirischen Forschung dieser Arbeit in Abschnitt 3.2 berücksichtigt wird.

Insbesondere wird die Determinante der *wahrgenommenen Benutzerfreundlichkeit*[42] für die in Abschnitt 3.3 beschriebene deduktive Inhaltsanalyse herangetragen und als eine Kategorie der strukturellen Untersuchung verwendet. Die zweite Hauptdeterminante *wahrgenommene Nützlichkeit* wird aufgrund der engen Bedeutungsähnlichkeit mit der Dimension der Funktionalität nicht explizit weiterverwendet, jedoch lässt sich aus der subjektiven Beschreibung einer Funktionalität die wahrgenommene Nützlichkeit ableiten.

Konkret werden die Erkenntnisse der Akzeptanzforschung für eine Bewertung vorgefundener Auswahlkriterien von Client Security Lösungen in Abschnitt 4.7 und Kapitel 5 genutzt. Mithilfe der aufgezeigten Mechanismen kann so abgeschätzt werden, welche Kriterien eine Akzeptanz auslösen können und welche eher nicht.

[39] Vgl. Lee/Kozar/Larsen 2003, S. 754 ff.
[40] Vgl. Gefen/Straub 2000, S. 8
[41] Vgl. Gefen/Straub 2000, S. 8 f.
[42] Der einfachen Prägnanz halber wird im weiteren Verlauf von *Benutzerfreundlichkeit* gesprochen. Der Bedeutung des Begriffs leitet sich weiterhin aus der Definition von Davis 1985 ab.

2.2 Technologieresistenz

Als logisches Gegenstück zu den Theorien der Akzeptanz kann das Konstrukt der Resistenz untersucht werden und damit eine ergänzende Betrachtungsweise zu den Ursachen individuellen Verhaltens ermöglicht werden.[43] Ähnlich wie beim Akzeptanzbegriff, finden sich in der Literatur verschiedene Verstehensansätze, welche einen Zugang zu dieser Thematik bereitstellen. Des Weiteren werden in der wissenschaftlichen Diskussion neben verschiedenen theoretischen Erklärungsansätzen auch empirisch belegte Ursachen der Resistenz genannt.

2.2.1 Resistenzbegriff

In der Literatur finden sich zwei verschiedene Verständnisse von Resistenz, wobei sich je nach Perspektive der Untersuchung verschiedene Definitionen von Resistenz ergeben. Einerseits wird die Resistenz als das Gegenstück von Akzeptanz und Adoption betrachtet.[44] Andererseits definieren verschiedene Studien, welche sich hauptsächlich auf organisatorische und umweltbedingte Faktoren beziehen, Resistenz als Folgeverhalten von Veränderungen.[45]

In Bezug auf den Gegensatz zur Akzeptanz wird Resistenz beispielsweise als mögliche Ursache angesehen, dass Technologie von einzelnen Nutzern oder Nutzergruppen nicht oder unvorteilhaft verwendet wird.[46] Allerdings wird Resistenz in diesem Kontext nicht ausschließlich als negativer und nicht konstruktiver Effekt von Individuen verstanden, sondern auch als ein effektiver Warn- und Schutzmechanismus beachtet, der den nicht zielführenden Einsatz von Technologie verhindert. Gründe für den nicht zielführenden Einsatz von Technologie können Stress der Mitarbeiter und eine Unterschreitung der angestrebten Leistungen sein.[47]

Exemplarisch für die verknüpfende Betrachtung mit Veränderung lässt sich die Resistenz von Mitarbeiter*innen gegenüber Informationstechnologie (IT) aus der Perspektive der Erwartungshaltung einer Gegenleistung der Individuen analysieren.[48] Dabei wird die Prämisse unterstellt, dass Individuen (beispielsweise Mitarbeiter*innen) gemäß des eigenen betriebenen Aufwands eine entsprechende Gegenleistung erwarten. Entspricht der wahrgenommene Wert der Gegenleistung nicht den Erwartungen des Individuums, so kann Resistenz entstehen.[49] Besonders augenscheinlich für die Betroffenen wird das Nichterfüllen der individuellen Erwartungshaltung durch eine Veränderung der Konstellationen aufgezeigt.

Um die Resistenz von Technologien untersuchen zu können erscheint die Berücksichtigung verschiedener Rahmenbedingungen als sinnvoll.[50] Zunächst muss festgestellt werden, welche

[43] Vgl. Markus 1983, S.
[44] Vgl. Markus 1983, S.
[45] Vgl. Joshi 1991, S. 229 ff.
[46] Markus 1983
[47] Markus 1983
[48] Vgl. Joshi 1991, S. 231
[49] Vgl. Joshi 1991, S. 231 f.
[50] Vgl. Samhan u. a. 2018, S. 3

Erwartungen und Anforderungen von welcher Benutzer*innengruppe ausgehen. Anschließend muss bestimmt werden, ob die Resistenz auf individuellem oder einem gruppendynamischen Level untersucht wird. Als dritte Rahmenbedingung sollte beachtet werden, auf welche Art und Weise die Einführung einer Technologie durchgeführt wird und welche Rolle den einzelnen Individuen in dieser Einführung zukommen.[51]

2.2.2 Zustandekommen von Resistenz

Einstellung und Verhalten der Resistenz werden in der Literatur seit kürzerer Zeit ebenso wie die Phänomene der Akzeptanz weniger intensiv erforscht. In dieser Arbeit werden dazu exemplarisch zwei verschiedene Modelle der Technologieresistenz vorgestellt.

Zur Ergründung der Bestandteile und der Dynamik von Resistenzen untersuchten Lapointe/Rivard die Art und Weise des Zustandekommens von Resistenz anhand verschiedener Fallanalysen und entwickelten auf ihren Ergebnissen aufbauend das in Abbildung 2 dargestellte Modell.[52] Im Zuge der in den Untersuchungen erhobenen Falldaten, welche zur Entstehung des Modells beigetragen haben, unterscheiden die Autoren in insgesamt sechs verschiedene Episoden der Resistenz, durch welche sich resistentes Verhalten eines Individuums charakterisieren lässt.[53] Das Verhalten wird dabei in einer zeitlichen Dimension der Episoden zu den empfundenen Bedrohungen der Individuen in Bezug gesetzt. Das Verhalten selbst wird als eine nach dem Grad der Resistenz geordneten Dimension dargestellt, welche am unteren Ende das Verhalten der Adoption abbildet und damit eine Schnittstelle zu den Akzeptanzmodellen aufzeigt.[54] Die Autoren gehen jedoch weder auf die Adoption noch auf die nächstresistentere Stufe der Neutralität ein und bilden diese damit nur theoretisch verortet ab. Daher wird auf eine weitere Erwähnung dieser beiden Episoden verzichtet und stattdessen die nächsthöheren Episoden in aufsteigender Reihenfolge des Resistenzverhaltens aufgelistet:

1. **Apathie:** In dieser ersten Stufe der Resistenz prägen Inaktivität und Desinteresse das Verhalten der Individuen gegenüber einer Technologie. Das Individuum verspürt eine Resistenz in Form von Frustration oder Verärgerung; weitere Verhaltensänderungen aufgrund von Resistenz werden in dieser Stufe nicht erwartet.[55]

2. **Passive Resistenz:** Auf der Apathie aufbauend drückt sich die passive Resistenz durch ein passiv-ablehnendes Verhalten wie die Nichtnutzung eines Systems aus.[56] Exemplarisch werden für diese Stufe Verhalten genannt, welche die Nutzung der ablehnenden Technologie ad absurdum führen und beispielsweise Verzögerungen im Arbeitsbetrieb oder eine Überlastung des Systems provoziert werden.[57]

[51] Vgl. Samhan u. a. 2018, S. 3
[52] Vgl. Lapointe/Rivard 2005, S. 483
[53] Vgl. Lapointe/Rivard 2005, S. 471 ff.
[54] Vgl. Lapointe/Rivard 2005, S. 472 f.
[55] Vgl. Lapointe/Rivard 2005, S. 473 f.
[56] Vgl. Lapointe/Rivard 2005, S. 474
[57] Vgl. Lapointe/Rivard 2005, S. 475 f.

3. **Aktive Resistenz:** Die nächsthöhere Stufe der Resistenz zeichnet sich durch eine aktiv-ablehnende Komponente aus, die bewusste Maßnahmen gegen die Nutzung der eingesetzten Technologie inspiriert.[58] Dieses Verhalten manifestiert sich beispielsweise in öffentlichen Empörungsbekundungen der Individuen oder durch den Zusammenschluss mehrerer resistenter Individuen mit der Intention, die eingesetzte Technologie zu beseitigen.[59]

4. **Aggressive Resistenz:** Als vollendete Stufe wird die Aggressive Resistenz genannt. Diese Form der Resistenz zeigt sich beispielsweise in dem Verhalten, Drohungen und Stimmungsmache gegen die eingesetzte Technologie zu verwenden, um neutrale Außenstehende von der Resistenz überzeugen und interne Machtkämpfe gewinnen zu können.[60]

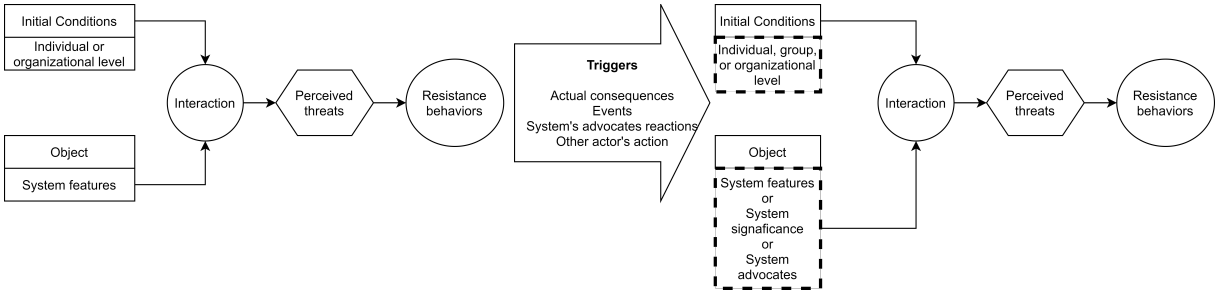

Abb. 2: Resistenzmodell nach Lapointe.[61]

Die genannten Ausprägungen des Resistenzverhalten stellen dabei ähnlich wie in den Untersuchungen von Akzeptanz die Folgen von bestimmten Faktoren dar. Neben dem vorgestellten, resultierenden Resistenzverhalten baut das in Abbildung 2 dargestellte Modell auf den folgenden Faktoren auf:

- **Initialbedingungen:** Anfängliche Zustände, welche als Trigger für das Resistenzverhalten fungieren, werden als Initialbedingungen zusammengefasst. Beispielweise können bestehende Machtverhältnisse, die Organisation oder bestimmte Arbeitsroutinen einen solchen Auslöser darstellen. Die Autoren weisen darauf hin, dass sich die Initialbedingungen mit dem zeitlichen Verlauf verändern können.[62]

- **resistent verhaltende Personen:** Das resistente Verhalten kann entweder von Individuen oder von dynamischen Gruppenkonstellationen ausgelebt werden. Beispielsweise können aktive und aggressive Resistenzverhalten bisher Außenstehende zur Resistenz anstiften. Die Autoren weisen darauf hin, dass ein resistentes Gruppenverhalten seinen Ursprung in resistent verhaltenden Einzelnen hat.[63]

[58] Vgl. Lapointe/Rivard 2005, S. 476
[59] Vgl. Lapointe/Rivard 2005, S. 476
[60] Vgl. Lapointe/Rivard 2005, S. 477 f.
[61] Mit Änderungen entnommen aus: Lapointe/Rivard 2005
[62] Vgl. Lapointe/Rivard 2005, S. 479
[63] Vgl. Lapointe/Rivard 2005, S. 480 f.

- **Gegenstand der Resistenz:** Das resistente Verhalten erfüllt nach Meinung der Autoren keinen Selbstzweck und ist daher immer gegen ein bestimmtes Objekt gerichtet. Im Fall der Technologieresistenz stellt dieser Gegenstand die Technologie dar; im Kontext dieser Arbeit könnten Resistenzen gegenüber Client Security Lösungen ergründet werden. Mit zeitlichem Verlauf der Nutzung einer Technologie kann sich das Objekt der Resistenz ändern. Lapointe/Rivard nennen exemplarisch das eingesetzte technologische System, dessen Bedeutung und die Befürworter des Systems als Objekte der Resistenz.[64]
- **Empfundene Gefahren:** Aus der Kombination der drei erstgenannten Faktoren bildet sich bei den Individuen und Gruppen ein Empfinden von subjektiven Gefahren aus. Analog zu dem im TAM genannten Faktor *Absicht zur Nutzung* leitet sich aus den empfundenen Gefahren das resistente Verhalten ab.[65]

Wie aus den Beschreibungen und der Abbildung 2 hervorgeht, bilden Initialbedingungen, die sich resistent verhaltende(n) Person(en) und das Objekt die ursachenlogische Basis für das Zustandekommen von resistentem Verhalten. Die Faktoren bedingen sich untereinander und führen in der Kombination zur Entstehung von empfundenen Gefahren. Aus diesen Gefahren lässt sich unmittelbar das resultierende resistente Verhalten ableiten. Das resistente Verhalten kann wiederum einen Ursprung für weitere resistente Episoden darstellen und führt entsprechend zu neuen oder veränderten Faktoren von Initialbedingungen, Subjekt und Objekt der Resistenz. Diese zeitliche, dynamische Komponente heben die Autoren immer wieder hervor und betonen, dass resistentes Verhalten einen auf Ursachen begründeten Status Quo darstellt und sich im zeitlichen Verlauf oder der Veränderung der Ausgangsfaktoren andere empfundene Gefahren und resistentes Verhalten ausprägen können.[66]

Der Zugang von Lapointe/Rivard (2005) ermöglicht die analytische Betrachtung von resistentem Verhalten, fokussiert sich jedoch auf die Untersuchung der dynamischen Elemente. Daher werden im folgenden Teil die Ursachen und möglichen Lösungsmittel der Resistenz betrachtet.

2.2.3 Konkrete Ursachen und Lösungsansätze der Resistenz

Neben den empfundenen Gefahren[67] werden in der Literatur weitere Ursachen für resistentes Verhalten aufgeführt, welche exemplarisch aufgelistet werden:

- **Statusverlust:** Individuen, im Kontext dieser Arbeit allen voran Mitarbeiter*innen, können einen Statusverlust erfahren, indem Aufgaben und Kernkompetenzen der Personen durch eine neu eingeführte Technologie übernommen werden und dadurch ein subjektives Empfinden schwindender Nützlichkeit und Wertschätzung auslöst.[68]

[64] Vgl. Lapointe/Rivard 2005, S. 480
[65] Vgl. Lapointe/Rivard 2005, S. 479 f.
[66] Vgl. Lapointe/Rivard 2005, S. 480 ff.
[67] Vgl. Lapointe/Rivard 2005, S. 478 ff.
[68] Siehe dazu: Vgl. Keen 1981, S. 28 f. und (Vgl. Joshi 1991, S. 234)

- **Machtverlust:** Insbesondere durch Veränderungen im Sozialgefüge kann es dazu kommen, dass Individuen einen Machtverlust wahrnehmen und somit die individuelle Autorität infrage gestellt sehen.[69] Es gilt dabei zu berücksichtigen, dass möglicherweise die Empfindungen der Personen nicht aus einer tatsächlichen Machtverschiebung hervorgehen und somit ein *falsches* Empfinden der Personen besteht. Dies ändert jedoch nichts an der Folge, dass ein resistentes Verhalten ausgelöst wird.[70]
- **Organisationelle Veränderungen:** Reorganisationen von Prozessen oder bestehender Arbeitsroutinen können aufgrund der Trägheit einzelner Individuen, sich nicht an neue Abläufe anpassen zu wollen, Resistenzen hervorrufen.[71]
- **Soziale Einflüsse:** Soziale Einflüsse können Individuen in ihrer Wahrnehmung beeinflussen, sodass bestimmte Eigenschaften einer neuen Technologie zu einer Adaption oder Resistenz führen können. Insbesondere ein eventuell vorhandener sozialer Druck kann neutrale, sich nicht akzeptierend oder resistent verhaltende, Personen zur Resistenz oder Akzeptanz treiben.[72]

Diesen möglichen Ursachen von Resistenz kann man mithilfe verschiedener Lösungsansätze gegensteuern. Beispielsweise kann eine offene Kommunikation helfen, stark subjektiv-verzerrte Empfindungen durch die Erläuterung der tatsächlichen Gegebenheiten, der Motivation und des erwarteten Nutzens zu berichtigen. Dadurch kann den betroffenen Personen ein Gefühl von Teilhabe vermittelt werden.[73] Außerdem kann diese offene Kommunikation durch eine dedizierte Integration der Individuen ausgebaut werden, sodass sich neue Aufgaben und Verantwortungen auf das subjektive Empfinden der Wertschätzung niederschlagen.[74] Abschließendes Beispiel der Lösungsansätze bilden Fortbildungen der Mitarbeiter*innen, wodurch das Verständnis und die Motivation der Nutzung gesteigert werden können, was wiederum ¬Resistenzen entgegen wirken kann.[75]

2.2.4 Nutzen für die weitere Arbeit

Die erschlossenen Erkenntnisse der Resistenzforschung ergänzen die Argumentation der Akzeptanzuntersuchungen und geben Hinweise darüber, aufgrund welcher Ursachen Resistenzeinstellungen und -verhalten entstehen. Außerdem etabliert insbesondere die Untersuchung von Lapointe/Rivard die verschiedenen Betrachtungsweisen auf Resistenz. Mithilfe der vorgestellten Ursachen und Mechanismen soll die Bewertung von Auswahlkriterien ermöglicht werden.

[69] Vgl. Markus 1983, S. 440 f.
[70] Vgl. Markus 1983, S. 440
[71] Vgl. Bhattacherjee/Hikmet 2007, S. 727 f.
[72] Vgl. Eckhardt/Laumer/Weitzel 2009, S. 18 f.
[73] Vgl. Land 1992, S. 150 f.
[74] Vgl. Leitch/Warren 2010, S. 192
[75] Vgl. Samhan u. a. 2018, S. 7

Greifbar werden die Ergebnisse dieses Abschnitts für eine Bewertung vorgefundener Auswahlkriterien von Client Security Lösungen in Abschnitt 4.7 und Kapitel 5 genutzt. Mithilfe der aufgezeigten Mechanismen kann so beurteilt werden, welche Kriterien eine Resistenz auslösen können.

2.3 Kriterien der ERP-Auswahl

In den vorherigen Abschnitten werden Akzeptanz und Resistenz als verhaltenswissenschaftliche Theorien der Technologieadaption beschrieben und aufgezeigt, wie mithilfe der Konstrukte eine Beurteilung von Client Security Lösungen ermöglicht werden kann. Dieser Teil der Arbeit geht der Frage nach, mithilfe welcher theoretischen Grundlagen eine differenzierte Analyse von Auswahlkriterien einer Client Security Lösung erfolgen kann. Aufgrund der Tatsache, dass Client Security Lösungen bisher wenig erforscht sind, wird die vorliegende Literatur zum Thema der ERP-Auswahlkriterien untersucht. ERP-Systeme sind bereits etablierte Lösungen, die in vielen verschiedenen Unternehmen Einsatz finden.[76] Durch das Hinzuziehen einer Vergleichsbasis in Form der ERP-Systeme, als bereits akzeptierte Client-Lösung in Unternehmen, sollen erste Kenntnisse in die fortlaufende Untersuchung dieser Arbeit miteinfließen können. Auf dieser Untersuchung aufbauend werden im Verlauf dieses Abschnitts abstrakte Dimensionen von Auswahlkriterien definiert, welche eine analoge Anwendung auf die Untersuchung Client Security Lösungen ermöglichen soll.

2.3.1 Wissenschaftlicher Stand

ERP-Systeme sind „integrierte Standardsoftwarepakete zur Abbildung von betriebswirtschaftlichen Prozessen in Organisationen“[77]. Sie können der Definition nach branchenübergreifend eingesetzt werden und stellen aufgrund der „Abbildung von betriebswirtschaftlichen Prozessen“[78] einen erfolgskritischen Faktor für Unternehmen dar. Der genannte Aspekt der Integration, welcher das ERP-System über Schnittstellen mit verschiedenen funktionalen Unternehmensbereichen verbindet, stellt die Einführung von ERP-Systemen als Herausforderung dar.[79] Insbesondere Planung, Testung und individuelle Anpassungen der ERP-Systeme konfrontieren einführende Unternehmen mit einem hohen personellen und zeitlichen Ressourcenbedarf, der die Auswahl eines ERP-Systems aufgrund des investierenden Charakters und der Höhe an möglichen Kosten komplex und schwierig gestalten kann.[80] Der hohe Bedarf an Ressourcen und möglicherweise angepassten eigenen Systemen gestalten das Revidieren eines einmal eingeführten ERP-Systems äußerst schwierig.[81]

[76] Vgl. Lepistö 2014, S. 194
[77] Vgl. Mauterer 2013, S. 7
[78] Vgl. Mauterer 2013, S. 7
[79] Vgl. Mauterer 2013, S. 10
[80] Vgl. Leyh 2016, S. 8
[81] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 794

Aufgrund der Wichtigkeit, infolge des hohen Ressourcenbedarfs und der Notwendigkeit eines verlässlichen Betriebs ein geeignetes ERP-System auszuwählen, wird das Verfahren der Auswahl intensiv erforscht.[82] Außerdem ist die Literatur durch die branchenunabhängigen Anwendungsmöglichkeiten der ERP-Systeme und durch die Problematik für kleine und mittelständige Unternehmen geprägt, sodass Forschungsarbeiten zu verschiedensten Anforderungsszenarien vorzufinden sind.[83]

Die intensive und breite Erforschung der ERP-Systeme geben den Ausschlag dazu, allgemeingültige Dimensionen der Technologieauswahl aus thematischen Abhandlungen der ERP-Auswahl abzuleiten. Dazu wird erstens unterstellt, dass sich bestimmte Dimensionen von Auswahlkriterien technologieübergreifend anwenden lassen. Zweitens argumentiert diese Arbeit mit der Prämisse, dass die breite Abdeckung[84] der Forschung von ERP-Systemen diese Ableitung aus der Literatur von ERP-Systemen zulässt. Beispielsweise werden dafür Sekundäruntersuchungen, wie Literature-Reviews, zu entwickelten Auswahlkriterien analysiert.[85] Drittens wird die Annahme vorausgesetzt, dass sich diese allgemeingültigen Dimensionen durch ihre Ausprägungen und ihre Wichtigkeit innerhalb der verschiedenen Anforderungsszenarien unterscheiden können.

2.3.2 Dimensionen der Auswahl

Wie bereits beschrieben, werden im Folgenden verschiedene Dimensionen der ERP-Auswahl beleuchtet, welche möglichst allgemeingültig für Technologieauswahlverfahren anwendbar sein sollen. Um die Festlegung auf die folgenden Dimensionen realisieren zu können, wird wie bereits erwähnt die vorhandene Literatur zu Auswahlkriterien von ERP-Systemen herangezogen. Jedoch erfolgt aufgrund der begrenzten Möglichkeiten im Rahmen dieser Arbeit keine quantitative Auswertung dieser Literatur nach der Häufigkeit genannter Dimensionen. Stattdessen werden die Dimensionen qualitativ begründet, und unter Berücksichtigung verschiedener Quellen, bestimmt. Ein Anspruch, alle relevanten Dimensionen berücksichtigt zu haben, besteht daher nicht, jedoch die Forderung der logischen Begründetheit, die zu der Berücksichtigung geführt haben. Im anschließenden Teil werden die bestimmten Dimensionen *Funktionalität*, *Anbieter*, *Interoperabilität* und *Kosten* vorgestellt, wobei die Ordnung in dieser Reihenfolge keine Priorisierung oder gesonderte Wichtigkeit einzelner Dimensionen darstellt. Dadurch, dass keine quantitative Qualitätsprüfung der Akzeptanzkriterien durchgeführt wird, wird im Zuge der Inhaltsanalyse nach Mayring[86], neben der beschriebenen deduktiven Vorgehensweise, die Möglichkeit offengehalten, weitere Kriterien induktiv bilden zu können. Dazu wird

[82] Vgl. Shehab u. a. 2004, S. 372
[83] Vgl. Shehab u. a. 2004, S. 360 ff.
[84] Gemeint ist hier der Bezug auf die Vielfältigkeit der untersuchten Anforderungsszenarien. Es wurden Untersuchungen bezüglich der Auswahl von ERP-Systemen beispielsweise für verschiedenste Branchen und Unternehmensgrößen durchgeführt. (Siehe dazu: Vgl. Shehab u. a. 2004, S. 360 ff. Vgl. Baki/Çakar 2005, S. 76 ff. und cite[Vgl.][S. 5 f.]Bernroider.2001
[85] Vgl. Baki/Çakar 2005, S. 76 ff.
[86] Vgl. Abschnitt 3.3

versucht, allen Expertenaussagen, die keiner der ERP-Dimensionen zugeordnet werden können, durch ein strukturiertes Reduktionsverfahren, einer neuen übergeordneten Kategorie des gleichen Abstraktionsniveaus zuzuordnen.

Funktionalität

Die Funktionalität gibt Aufschluss über den Zweck und die Anwendungsmöglichkeiten einer technischen Lösung. Bei ERP-Systemen äußert sich diese Funktionalität beispielsweise durch die Integrationstiefe von ERP-System und verschiedenen funktionalen Arbeitsbereichen oder die Kombinationsmöglichkeiten einzelner Module des Systems. Als spezifische Funktionen von ERP-Systemen werden die Integration der Supply-Chain, das Bestellmanagement, Datenverwaltung und Vertriebsautomation exemplarisch genannt.[87]
Für ERP-Systeme ist außerdem die Vollständigkeit der funktionalen Abdeckung ein wichtiges Kriterium der Auswahl.[88] Diese Abdeckung kann durch die Berücksichtigung aller funktionalen Unternehmensbereiche, wie zum Beispiel Personalabteilung, Materialmanagement, Projektmanagement und Produktionsplanung erfolgen.[89] Zusammenfassend lässt sich die Funktionalität von ERP-Systemen in der Betrachtung von drei Aspekten analysieren: *Funktionale Bereiche*, welche durch die Lösung abgedeckt werden, die *Flexibilität hinsichtlich einer Anpassung* (Customizing) und *Offenheit der Lösung* und spezifische Eigenschaften, die für ein ERP-System Voraussetzung sind.[90] Aus den aufgeführten Überlegungen zur Funktionalität lässt sich ableiten, dass die Funktionalität den Einsatzzweck einer Lösung begründet und damit deren Existenzberechtigung und den tatsächlichen Nutzen, der aus einer Anwendung hervorgehen kann, bestimmt.[91] Dieser These folgend wurde bei einer Untersuchung von zwanzig ERP-Projektmanager*innen kanadischer Unternehmen festgestellt, dass die Funktionalität bei der Auswahl eines ERP-Systems mit 79 % den wichtigsten Faktor für die befragten Personen darstellt.[92]

In Bezug auf die Anwendung dieser Dimension auf die Untersuchung von Auswahlkriterien der Client Security Lösungen, stellt sich die Frage, welche spezifischen Funktionen eine Client Security Lösung auszeichnen und inwiefern sich die Funktionalität auf weitere Kriterien auswirkt. Insbesondere die Aspekte der Vollständigkeit und Anpassungsmöglichkeiten dienen der Untersuchung als Grundlage. Client Security Lösungen sind in ihrer Funktionalität durch den Zweck des Client-Schutzes definiert, sodass in der Forschung dieser Arbeit herauszufinden gilt, welche funktionalen Rahmenbedingungen diesen Schutz gewährleisten.

Entsprechend gilt es im Verlauf dieser Arbeit festzustellen, welche funktionalen Komponenten die Client-Sicherheit gewährleisten und wie sich diese Funktionalität im Detail äußert. Das

[87] Vgl. Shehab u. a. 2004, S. 360
[88] Vgl. Baki/Çakar 2005, S. 77
[89] Vgl. Baki/Çakar 2005, S. 77
[90] Vgl. Illa/Franch/Pastor 2000, S. 117
[91] Ein Verknüpfung von Nützlichkeit und tatsächlicher Nutzung findet sich in TAM (siehe dazu Abschnitt2.1)
[92] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 797

Verständnis dieser Dimension wird durch die folgende Fragestellung ausgedrückt:

Was soll die Lösung können?

Anbieter

Der Anbieter ist der Leistungserbringer und nimmt in der ERP-Auswahl aufgrund der Oligopolstellungen einiger Anbieter einen zentralen Aspekt ein.[93] Aufgrund des erwähnten hohen Ressourcenbedarfs wird eine langfristige Nutzung eines ERP-Systems angestrebt, welche entsprechend eine verlässliche Zusammenarbeit mit einem Anbieter erfordert.[94] Weitere Gründe für die Wichtigkeit des Anbieters ergeben sich daraus, dass ERP-Systeme meistens als Dienstleistungen angeboten werden und daher eine beständige Pflege der Aktualität und Funktionalität durch den Anbieter geschehen muss. Außerdem werden im Rahmen eines ERP-Systems viele modulare Funktionen angeboten, aus denen Kund*innen entsprechend ihrer Bedürfnisse eine Kombination auswählen. Mit der Wahl des Anbieters geht so auch der Umfang der wählbaren Module einher und die Möglichkeit zukünftig erweiternde Funktionen zu integrieren.[95]

Konkret werden in Untersuchungen der Anbieterkriterien einer ERP-Auswahl die Anbieterunterstützung[96], Marktposition des Anbieters[97], das Anbieterimage[98], Referenzen des Anbieters[99] und das Domänenwissen des Anbieters[100] genannt.

Bezüglich der Anwendung dieser Dimension auf die Untersuchung der Auswahlkriterien einer Client Security Lösung, könnte sich aufgrund des Sicherheitsaspekts, durch welchen den Lösungen teilweise weitreichende Berechtigungen durch Zugangssperrungen und weiteren präventiven Interventionen zukommen, herausstellen, dass das Domänenwissen oder die Marktposition die entsprechende Kompetenz eines Anbieters herausstreichen und als wichtiges Kriterium angesehen werden.

Bei all diesen Ausführungen der Wichtigkeit des Anbieters, die vor allen Dingen auf der zukünftigen Verlässlichkeit der Produktfunktionalität begründet wird, stellt sich doch die Frage, inwiefern dieser Zusammenhang zwingend bestehen muss und beispielsweise die Zukunftsfähigkeit eines Produkts nicht auch auf andere Weise gewährleistet werden kann. Im Kontext der Client Security Lösungen und dieser Arbeit ergibt sich somit ein Informationsbedarf, die für die Kund*innen relevanten Eigenschaften eines Anbieters herauszuarbeiten und insbesondere die Motivation herauszufinden, welche zu der Auswahl der Eigenschaften führt.

[93] Siehe dazu: Vgl. Mauterer 2013, S. 13 f. und Vgl. Shehab u. a. 2004, S. 365
[94] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 794
[95] Vgl. Illa/Franch/Pastor 2000, S. 117
[96] Vgl. Bernroider/Koch 2001, S. 5, Vgl. Everdingen/Waarts 2003, S. 22
[97] Vgl. Bernroider/Koch 2001, S. 5
[98] Vgl. Everdingen/Waarts 2003, S. 22
[99] Vgl. Baki/Çakar 2005, S. 80
[100] Vgl. Rao 2000, S. 87

Die Beantwortung dieses Informationsbedarfs wird durch die folgende Fragestellung geleitet:

> *Mit welchen Eigenschaften soll der Anbieter Betrieb und Implementierung der Lösung unterstützen und wieso soll er das tun?*

Interoperabilität

Die Interoperabilität bezeichnet den Grad eines Produkts, mit anderen Systemen, Produkten oder Komponenten kompatibel zusammenarbeiten zu können.[101] Die Kompatibilität lässt sich dabei über die Kommunikationsfähigkeit zweier Systeme, der technisch-funktionalen Schnittstellen bis auf die hardware-nahe Ebene der Datenübertragung auf verschiedenen technischen Ebenen betrachten.[102] Aus der Definition ergibt sich, dass der Datenaustausch als Indikator der Interoperabilität auf Empfänger- wie auf Senderseite mittels definierter Schnittstellen zu berücksichtigen ist.[103] Bei der Einführung neuer Lösungen und Systeme stellt dies eine Sondersituation dar. Die neue Lösung muss gemäß den Anforderungen des einführenden Unternehmens zu den vorhandenen Schnittstellen der bereits implementierten Systeme und Lösungen passen – also kompatibel sein. Daraus leitet sich ab, dass die geforderte Interoperabilität einer neuen Lösung von der vorhandenen Architektur an Lösungen und Systemen abhängt und in welcher Weise eine neue Lösung mit diesen kollaborieren soll. In der Literatur wird auch der Ausdruck der „Application Integration“[104], „fit with parent/allied organization systems“[105] anstelle der Interoperabilität verwendet. In der bereits angeführten Studie von Kumar, V./Maheshwari/Kumar, U. (2003) wurde festgestellt, dass das Kriterium der „Fit with parent/allied organisation systems“[106] als drittwichtigstes Kriterium für die Auswahl von ERP-Systemen galt.[107] Für ERP-Systeme werden in der Literatur in Bezug auf die Interoperabilität die Kriterien Integrationsmöglichkeiten[108], Möglichkeiten der Anpassung[109] und die Abbildung geschäftlicher Prozesse[110] genannt. Eine mangelnde Interoperabilität innerhalb der IS eines Unternehmens kann zu koexistierenden Applikationen, welche dieselben oder ähnliche Funktionen ermöglichen, führen.[111]

In der Betrachtung von Client Security Lösungen gilt es zu prüfen, welche Rolle der Interoperabilität zukommt und anhand welcher Kriterien die Fähigkeit zur Interoperabilität einer Client Security Lösung bestimmt werden kann. Beispielsweise könnte sich die Interoperabilität durch

[101] Vgl. International Organization for Standardization 2011
[102] Vgl. International Organization for Standardization 2011
[103] Vgl. International Organization for Standardization 2017
[104] Vgl. Themistocleous u. a. 2001, S. 2
[105] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 797
[106] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 797
[107] Vgl. Kumar, V./Maheshwari/Kumar, U. 2003, S. 797
[108] Vgl. Linthicum 2000, S. 3 ff.
[109] Vgl. Themistocleous u. a. 2001, S. 1
[110] Vgl. Everdingen/Waarts 2003, S. 10
[111] Vgl. Themistocleous u. a. 2001, S. 1 f.

die Vorgabe bestimmter, standardisierter Schnittstellen vorgegeben werden. Außerdem könnte der Interoperabilität von Client Security Lösungen ein besonderer Stellenwert zukommen, da manche Lösungen die Aktivitäten anderer Systeme einerseits überwachen und andererseits aktiv kontrollieren. Für die Ermöglichung dieser Funktionalität ist eine entsprechende Interoperabilität der Lösung eine Voraussetzung.

Um die Dimension der Interoperabilität bei Client Security Lösungen betrachten zu können, wird sich an der folgenden Leitfrage orientiert:

> *Wie soll die Lösung die Funktionalität erfüllen?*

Kosten

Die Kosten spielen in der Auswalbetrachtung eine limitierende Rolle und definieren oftmals den Rahmen der Produkteigenschaften.[112] Bezahlbarkeit der ERP-Systeme ist ein Kriterium der Kosten, wobei die Bezahlbarkeit sich aus der Relation von anfallenden Kosten und den Eigenschaften der Technologie ergeben.[113] Hinsichtlich der verschiedenen Arten von anfallenden Kosten erweisen sich großzügige Schätzungen für Implementierungs- und Wartungskosten als hilfreich. Denn viele ERP-Einführungen scheitern oder es entstehen während der Einführung unvorhergesehene Probleme, welche sich nur kostenintensiv beheben lassen.[114] Neben den genannten Kosten können Betriebskosten für Lizenzen und Anschaffungskosten für benötigte Software, Hardware und Fortbildung anfallen.[115]

In Bezug auf die Kostenuntersuchung bei Client Security Lösungen gilt es herauszufinden, welche Art von Kosten für die Auswahl entscheidend sind. Außerdem wird analysiert werden, durch welche Vorgaben die tragbaren Kosten definiert werden. Beispielsweise könnte es sich bei Client Security Lösungen ähnlich verhalten, wie bei ERP-Systemen, sodass die Investitionen für Planung, Testung und Implementierung relativ hoch veranschlagt werden, um den Erfolg einer komplexen Einführung und den funktionierenden Betrieb zu ermöglichen.

Die Dimension der Kosten wird in der weiteren Arbeit durch Heranziehen der folgenden Fragestellung betrachtet werden:

> *Mit welchen Ressourcen soll die Lösung betrieben werden und wofür sollen diese verwendet werden?*

[112] Vgl. Baki/Çakar 2005, S. 79
[113] Vgl. Rao 2000, S. 87
[114] Vgl. Themistocleous u. a. 2001, S. 2
[115] Vgl. Baki/Çakar 2005, S. 79

2.3.3 Nutzen für die weitere Arbeit

Die in diesem Abschnitt vorgestellten Dimensionen der ERP-Auswahl werden in der weiteren Arbeit analog zu der differenzierten Betrachtung von Client Security Lösungen angewendet. Konkret werden die Dimensionen dabei in der Erstellung des Interviewleitfadens (Abschnitt 3.2) verwendet und in der deduktiven Inhaltsanalyse als Kategorien zur Strukturierung des erhobenen Datenmaterials herangetragen und dienen der Erstellung des Kodierleitfadens[116].[117]

Des Weiteren werden die Dimensionen in der Evaluierung von HP Sure Admin als Betrachtungsgrundlage verwendet und unterstützen damit eine strukturierte und fundierte Bewertung.

In diesem Kapitel wird der Begriff *Dimension* für eine abstrakte Zusammenfassung mehrerer kontext-ähnlicher Auswahlkriterien verwendet. Der Dimensionsbegriff ermöglicht damit einen öffnenden Ansatz, worin sich die unterschiedliche Ausgestaltung der kontext-ähnlichen Kriterien ausdrückt und die Menge an möglichen Kriterien aufzeigt. Im weiteren Verlauf wird dagegen von *Kategorien* die Rede sein, um den eingrenzenden Charakter der Auswertung hervorzuheben und die Nomenklatur Mayrings zu verwenden.

[116] Vgl. Abschnitt 3.5
[117] Vgl. Mayring 2015, S. 67 f.

3 Methodik

Zielsetzung: In diesem Kapitel wird das Forschungsdesign beschrieben. Die Zielsetzung besteht darin, die Vorgehensweise in der Beantwortung der Forschungsfrage dieser Arbeit zu beschreiben und zu erläutern. Mit der Festlegung eines Forschungsdesigns wird das Ziel verfolgt, den strukturellen Aufbau der Zielerreichung zu fixieren und die Kontrolle des Verfahrens zu gewährleisten.[118] Während in der quantitativen Forschung die Gütekriterien Reliabilität, Validität und Objektivität weitestgehend anerkannt sind, werden in der Literatur unterschiedliche Gütekriterien qualitativer Sozialforschung diskutiert.[119] Dieser Diskurs lässt sich primär auf die mangelnde granulare Standardisierung der Erhebungssituationen qualitativer Forschung zurückführen, sodass der Anspruch nach Reliabilität und Validität erschwert wird und teilweise dem offenen Charakter qualitativer Methoden widerspricht.[120] Aufgrund dieser Unstimmigkeit und der begrenzten Möglichkeiten im Rahmen der vorliegenden Arbeit diesen beiden Gütekriterien gerecht zu werden, wird mithilfe dieses Kapitels versucht, zumindest die Güte der Transparenz in dieser Forschungsarbeit erfüllen zu können.[121] Zentraler Anspruch ist es dabei, die Methodik transparent vorzustellen, sodass eine logische wie inhaltliche Nachvollziehbarkeit und Bewertung des angewandten Vorgehens ermöglicht werden.

Aufbau: Zu Anfang dieses Kapitels findet eine Erläuterung des Forschungsdesigns statt, die aufzeigt, mittels welcher Forschungsmethoden die Beantwortung der Forschungsfrage angestrebt wird. Im darauffolgenden Abschnitt wird das empirische Erhebungsinstrument der Experteninterviews als Teil der qualitativen Forschung herangezogen. Darin erfolgt einerseits die Beschreibung und Begründung des Interviewleitfadens und mit welcher Ergebnisintention die Interviews durchgeführt werden. Andererseits wird festgehalten, anhand welcher Kriterien die Selektion der Interviewpartner stattfinden wird und wie die Interviewpartner in ihrem spezifischen Kontext charakterisiert werden können. Im dritten Teil des Kapitels werden Varianten der qualitativen Datenauswertung diskutiert und das gewählte Auswertungsverfahren detailliert vorgestellt. Der vierte Abschnitt thematisiert als ersten Verarbeitungsschritt der erhobenen Daten die Transkription der Experteninterviews. Abschließend erfolgt eine Erläuterung des im Rahmen der Auswertung angewandten Kodierleitfadens.

3.1 Forschungsdesign

Das Forschungsdesign prägt den Aufbau, Vorgehen und Inhalt dieser Arbeit und stellt damit einen fundamentalen qualitativen Aspekt dar. Den Ausgangspunkt der Forschung liefert die in Kapitel 1.3 vorgestellte Forschungsfrage:

[118] Vgl. Flick 2009, S. 77
[119] Vgl. Flick 2020, S. 247 f.
[120] Vgl. Flick 2020, S. 249 f.
[121] Vgl. Mayring 2020, S. 4 f.

Verfahren	Literaturrecherche	Experteninterviews zur empirischen Erhebung	deduktiv-qualitative Analyse
Zielsetzung	theoretische Einordnung, Erfassen vorhandener Lösungsansätze	fachspezifisches Wissen sammeln, Rekonstruktion der Auswahlsituation	Analyse & Interpretation erhobener Daten, Beantwortung der Forschungsfrage
Verortung in der Arbeit	2. Kapitel	3. Kapitel	4. Kapitel

Tab. 1: Überblick des Forschungsdesigns, der Zielsetzungen und der Aufbereitung in der schriftlichen Ausarbeitung.

*Welche Nutzenpotenziale und Resistenzfaktoren stehen sich bei der Entscheidungsfindung von Kund*innen zum Einsatz einer Client Security Lösung gegenüber?*

Wie das in Tabelle 1 abgebildete Forschungsdesign zeigt, findet zu Beginn eine Untersuchung der wissenschaftlichen Literatur statt, womit eine thematische Einordnung der Forschungsfrage und eine Einschätzung des vorhandenen theoretischen Deskriptions- und Explikationsrahmens bezweckt werden sollte. Dieser Schritt erfolgte in Kapitel 2 und zeigt einerseits auf, welche Rolle die Akzeptanz und Resistenz von Individuen in der Technologieauswahl von Unternehmen spielen. Andererseits wurden anhand der ausführlich untersuchten Auswahlkriterien von ERP-Systemen Dimensionen aufgestellt, welche einen Betrachtungsrahmen für die Analyse der Auswahlsituationen von Client Security Lösungen bilden.

Auf dieser literarischen Untersuchung aufbauend kann eine fundierte Strategie für die Beantwortung der Forschungsfrage erstellt werden. In der vorliegenden Forschungsfrage wird der Untersuchungsgegenstand, die Client Security Lösung, aus der Perspektive von Kund*innen untersucht. Da in der Literatur kaum Hinweise auf die Auswahlkriterien von Client Security Lösungen zu finden sind, werden als Grundlage für die Untersuchung Dimensionen der Auswahlkriterien von ERP-Systemen herangezogen. Aus diesen Dimensionen lassen sich Fragestellungen für eine empirische Erhebung im Rahmen dieser Arbeit ableiten, die der Erforschung von Client Security Lösungen dient. Die empirische Untersuchung der Entscheidungsfindung und des Handelns der Kunden*innen stellt einen verhaltenswissenschaftlichen Gegenstandsbereich der Sozialforschung dar, da die Sozialforschung dem Bestreben folgt, das Handeln von Individuen „in seinem Ablauf und in seinen Wirkungen ursächlich zu erklären“[122]. Die Ursachen dieser individuellen Handlungen werden dabei gemäß der Forschungsfrage in Nutzenfaktoren und Resistenzfaktoren bei Auswahl von Client Security Lösungen differenziert. Dies ergänzend wird in dieser Arbeit der Ansatz verfolgt, die abstrakten Dimensionen der ERP-Auswahl analog für die Einteilung der Auswahlkriterien von Client Security Lösungen heranzuführen und die Beziehungen der einzelnen Faktoren untereinander und deren tatsächliches

[122] Gläser/Laudel 2009, S. 24

Wirken auf den Entscheidungsprozess einzelner Individuen durch den Einbezug von Akzeptanz und Resistenz zu beschreiben.

In der empirischen, auf Realitätsbeobachtungen beruhenden, Sozialforschung werden grundsätzlich die zwei Extreme der qualitativen und der quantitativen Forschung unterschieden, wobei in der Praxis oft eine Vermischung der beiden Extreme zu beobachten ist.[123] Quantitative Forschung dient dabei eher theorieprüfenden Untersuchungen, deren Aussagekraft sich in der Verallgemeinerung und auf mathematischen Analysen von meist vielen Einzelfällen begründet. Demgegenüber charakterisiert sich die qualitative Forschung durch einen hypothesengenerierenden Ansatz, der in der Struktur eher offener gestaltet ist, um einen freien Interpretationsspielraum zu gewähren und auf diese Weise Wissen zu generieren.[124]

Quantitative Verfahren setzen standardisierte Datenerhebungen ein, um bestehende Theorien über bestimmte Kausalzusammenhänge zu überprüfen und den wissenschaftlichen Ansatz der Falsifizierung umzusetzen.[125] Qualitative Verfahren hingegen suchen nach bisher unbekannten Kausalmechanismen und bedienen sich typischerweise eines oder weniger Fälle als Grundlage der Untersuchung. Dadurch können die qualitativen Verfahren keine Aussage über die Breite der Anwendbarkeit des generierten theoretischen Wissens treffen.[126]

Vor diesem Hintergrund bieten sich diejenigen verhaltenswissenschaftlichen Methoden zur Erhebung von Daten an, welche einerseits eine Berücksichtigung vorhandenen Wissens erlauben und andererseits einen, dem wenig erforschten Untersuchungsgegenstands der Client Security Lösungen angemessenen, offenen Antwortrahmen ermöglichen.

Durch eine derartige Kombination theoretischen und empirischen Wissens sollen die Ergebnisse dieser Forschungsarbeit einerseits neues Wissen festhalten und andererseits eine Einordnung in das Gefüge der wissenschaftlichen Forschung zulassen.[127]

Im folgenden Abschnitt wird begründet, weshalb sich auf die Methode der halbstrukturierten Experteninterviews festgelegt wird und inwiefern dieser Ansatz dem beschriebenen Anspruch gerecht werden kann. In Abschnitt 3.3 wird die geeignete Auswertung der erhobenen Interviewdaten als letzter Schritt des Forschungsdesigns thematisiert, bevor in Kapitel 4 die Ergebnisse der qualitativen Auswertung beschrieben und diskutiert werden.

3.2 Experteninterviews als Methode der empirischen Erhebung

Auch bei Experteninterviews können quantitative und qualitative Vorgehensweisen kombiniert werden, sofern sich dieser Ansatz für die Untersuchung eignet. Im Rahmen dieser Forschungsarbeit wird jedoch eine rein qualitative Untersuchung angestrebt, da diese zur explo-

[123] Vgl. Gläser/Laudel 2009, S. 25
[124] Vgl. Gläser/Laudel 2009, 12 f.
[125] Vgl. Gläser/Laudel 2009, 26 f.
[126] Vgl. Gläser/Laudel 2009, 25 f.
[127] Vgl. Gläser/Laudel 2009, S. 24

rativen Grundlagenforschung von Auswahlkriterien der Client Security Lösungen beitragen soll.[128] Als eine qualitative Erhebungsmethode bieten sich Experteninterviews sowohl für detaillierte Rekonstruktionen von fachkundigen Spezialist*innen als auch für die „Erfassung von Deutungen, Sichtweisen und Einstellungen der Befragten selbst“[129] an. Experteninterviews lassen sich in unterschiedlicher Ausprägung durch die Gestaltung eines Leitfadens standardisieren. Ein Vorgehen ist dabei die Verwendung eines halb-standardisierten Leifadens, welcher spezifische Fragen als Struktur vorgibt und in der Anwendung durch zusätzliche Fragen ergänzt werden kann.[130] Die freiere Fragestellung führt einerseits zu einer geringeren Vergleichbarkeit der verschiedenen Interviews, andererseits können spezifische Auffälligkeiten detaillierter erschlossen werden und unter Umständen in die Leitfäden künftiger Interviews miteinfließen.[131]

Da halb-standardisierte Leitfäden die Vorteile der Standardisierung mit der Ergebnisoffenheit verbindet und damit im Sinne qualitativer Forschung neuartiges Wissen rekonstruierend erschlossen werden kann, wird diese Form der Experteninterviews in dieser Arbeit verwendet.

Leitfaden

Bei der Erstellung des Leitfadens werden zwei Aspekte für die allgemeine Fragenformulierung berücksichtigt. **Erstens** wird viel Wert daraufgelegt, die Fragen an die Experten*innen in dem Maße zu stellen, dass Antworten in Form von rekonstruktiven Beschreibungen zu erwarten sind. Dies wurde einerseits dadurch angestrebt, dass die Fragen lediglich mithilfe des Erfahrungs- und Kompetenzschatzes der befragten Person beantwortet werden können und keine Spekulationen initiiert werden. Andererseits wird darauf geachtet, möglichst neutrale Fragen zu stellen, in dem Sinne, dass der befragten Person keine richtige oder falsche Antwort beziehungsweise eine Erwartungshaltung des Interviewenden suggeriert wird. Dies führt entsprechend zu einer eher offenen Fragendogmatik, die der befragten Person viel Spielraum in der Beantwortung der Fragen lässt. Ein Ausmaß großen Spielraums der Antworten kann sich problematisch auf die Vergleichbarkeit der Interviews auswirken, sodass untergeordnete Fragen zur Spezifizierung unkonkreter Antworten in den Leitfaden aufgenommen werden.

Zweitens wird versucht das Gütekriterium der Triangulation[132] innerhalb eines Interviews zu erfüllen, indem sich verschiedene Fragen auf dieselben Untersuchungsgegenstände beziehen und damit mehrere Themenzugänge kombiniert werden.[133] Exemplarisch dafür wurden die Expert*innen gebeten, die zuletzt eingeführte oder beurteilte Client Security Lösung vorzustellen. Anhand dieser spezifischen Lösung werden Fragen gestellt, welche die Rolle der in

[128] Vgl. Bortz/Döring 2006, S. 314
[129] Hopf 2016, S. 17
[130] Vgl. Saunders/Lewis/Thornhill 2009, S. 323
[131] Vgl. Berger-Grabner 2016, S. 140
[132] Triangulation bezeichnet das Vorgehen, mithilfe verschiedener Perspektiven den Untersuchungsgegenstand zu erforschen, und verfolgt das Ziel, einen Erkenntnisgewinn generieren zu können. (Vgl. Flick 2011, S. 10)
[133] Vgl. Flick 2020, S. 190 f.

Abschnitt 2.3 beschriebenen Dimensionen in der Auswahl und Entscheidung für das benannte Produkt ergründen. Den zweiten Teil der Triangulation bildet der Fragenteil über einen möglicherweise vorhandenen Prozess zur Einführung und Auswahl von Client Security Lösungen. Falls die befragte Person die Existenz eines solchen Prozesses bejahen kann, so wird die Rolle der in Abschnitt 2.3 beschriebenen Dimensionen für den Verlauf und das Ergebnis des Prozesses durch entsprechende Fragen untersucht. Mithilfe dieses Ansatzes können aus den Diskrepanzen zwischen einem vorhandenen Prozess und einem manifestierten Produktbeispiel Hinweise auf unterbewusste oder zumindest nicht prozessual berücksichtige Faktoren abgeleitet werden.

Zu Anfang des Interviews wurden die Expert*innen gebeten, ihr Unternehmen und ihren Verantwortungsbereich zu erläutern. Im Zuge dessen wurden beispielsweise auch die Anzahl der betreuten Clients bestimmt und die Quellen der unternehmenseigenen Sicherheitsanforderungen ergründet.

Der zweite Abschnitt dient hauptsächlich der rekonstruierenden Beschreibung einer exemplarischen Client Security Lösung und deren Auswahlsituation. Zunächst werden die Expert*innen nach Beispielen für den Einsatz von Client Security Lösungen in ihrem Unternehmen befragt. Anschließend werden anhand der zuletzt eingeführten Client Security Lösung Fragen über die Rolle der Dimensionen (Anbieter, Kosten, Interoperabilität, Funktionalität, Benutzerfreundlichkeit) in der spezifischen Auswahl gestellt. Um die Wichtigkeit der Kriterien grob beleuchten zu können, wird anschließend die Frage gestellt, was den Ausschlag für die Auswahl der Lösung gegeben hat.

Im dritten Abschnitt wird ein möglicher Prozess zur Auswahl und Entscheidung von Client Security Lösungen thematisiert und erfragt, wer darin beteiligt ist und wie dieser abläuft.

Im vierten Teil des Leitfadens werden allgemeingültige Auswahlkriterien der Client Security Lösungen und deren Wichtigkeit anhand der definierten Dimensionen erfragt. In diesem Abschnitt wird außerdem die äußerst subjektive und nicht rekonstruierende Frage gestellt, was nach Meinung der befragten Person, eine Client Security Lösung in ihrem Einsatz bezwecke. Die Frage sollte einen Aufschluss darüber geben, welche Stellung Client Security Lösungen in der Unternehmensumgebung einnehmen und welche grundlegende Erwartungshaltung damit einhergeht.

Im abschließenden Abschnitt wird das BIOS eines Clients als spezifischer Untersuchungsgegenstand von *HP Sure Admin* thematisiert. Hier werden Fragen gestellt, die den Status Quo der BIOS-Sicherheit im Unternehmen beschreiben sollen und Aufschluss über das Vorgehen und das Management ergeben. Zum Schluss wird die hypothetische Frage gestellt, wie nach Meinung der befragten Person der ideale BIOS-Schutz aussehen soll. Die Antworten auf diese Frage sollen Klarheit über die Eigenschaften des BIOS, die besonders wünschenswert sind, geben. Auf Basis dessen soll erkennbar werden, welche Aspekte an der aktuellen Situation des BIOS-Schutzes noch verändert werden sollen und welche Entwicklung die Befragten in der Zukunft erwarten.

Auswahl der Expert*innen

Die Auswahl einer Zielgruppe der Forschung grenzt einerseits die möglichen erwartbaren Erkenntnisse der Interviews ein. Andererseits gewährleistet eine spezifische Eingrenzung die Vergleichbarkeit der Expert*innen und damit eine übergreifende inhaltliche Analyse.[134] Es wurden folgende Kriterien festgelegt, um Expert*innen zu definieren:

- Expert*in ist bei einem Geschäftskunden von HP beschäftigt.
- Expert*in hat Erfahrungen mit Client Security Lösungen im alltäglichen Umgang gemacht.
- Expert*in hat Einblick in Auswahl- und oder Entscheidungsverfahren von Client Security Lösungen oder benutzt diese in hoher Häufigkeit.
- Expert*in arbeitet seit mindestens drei Jahren in der beruflichen Rolle oder hat andere Eigenschaften, welche eine angemessene Kompetenz indizieren.

Des Weiteren wird versucht, verschiedene Unternehmen mit möglichst heterogenen Eigenschaften wie Branche und Sicherheitsanforderungen in der Erhebung zu berücksichtigen, um Antworten aus unterschiedlichen Unternehmensperspektiven zu erhalten. In zwei Unternehmen können je zwei Expert*innen gewonnen werden, sodass neben der beschriebenen methodeninternen Triangulation versucht wird, zumindest wenige Rekonstruktionen mittels Datentriangulation verschiedener Expert*innen auf Differenzen und Gemeinsamkeiten zu überprüfen. Die Datentriangulation verbindet verschiedene Datenquellen, welche sich in der Erhebung in Bezug auf Zeit, Ort oder befragter Person unterscheiden.[135] Einerseits können mithilfe dieser Triangulation und der Feststellung der Unterschiede womöglich subjektiv geprägte Verhalten und Sichtweisen identifiziert werden, welche selbst, wenn sie nicht interpretierbar, wenigstens auffällig sind und für die Betrachtung der Validität herangezogen werden können. Andererseits kommen Ansätze der Triangulation häufig zu dem Ergebnis, dass sich die Daten verschiedener Perspektiven komplementär ergänzen und dadurch ein höherer Grad an vollständiger Rekonstruktion erreicht wird, was ebenso dem Erkenntnisgewinn dienlich ist.[136]

Rolle des Forschers im qualitativen Forschungsprozess

Ein Aspekt der qualitativen Forschung ist die Kommunikation und Interaktion zwischen den Untersuchungsteilnehmern, die aufgrund des subjektorientierten Forschungsprozesses als eine mögliche Manipulations- und Erkenntnisquelle betrachtet wird.[137] Vor diesem Hintergrund

[134] Vgl. Mayer 2008, S. 39 f.
[135] Vgl. Flick 2020, S. 189
[136] Vgl. Flick 2020, S. 192 f.
[137] Vgl. Bortz/Döring 2006, S. 304 f.

soll das Setting der Interviewsituationen transparent geschildert werden, um eine Einschätzung zu ermöglichen, inwiefern eine Beeinflussung der Teilnehmenden durch den Forschenden besteht.[138] Alle Interviews werden über digitale Videoanrufe durchgeführt, wobei sich die Teilnehmenden sowie der Forschende in einer privaten Arbeitsumgebung im *Homeoffice* befinden. Die Teilnehmenden und der Forschende kennen sich vor Beginn des Interviews nicht und haben davor lediglich bezüglich der Vereinbarung des Interviewtermins und der Einwilligungserklärung der Teilnehmenden kommuniziert. Um dem Interview einen dialog-ähnlichen Charakter zu verleihen, ein erstes Vertrauen zwischen Teilnehmer*in und Forscher herzustellen und die teilnehmende Person in eine „vertraute Kommunikationssituation"[139] zu versetzen, wird das Gespräch mit neutralen, interviewunabhängigen Themen begonnen.[140]

Ablauf

Anschließend beginnt das Interview mit der Vorstellung des Forschungsthemas, der Erklärung der Zielsetzung der Interviews und einem letzten Hinweis zur Einwilligungserklärung. Danach wird die Aufnahme der Interviews gestartet und die erste Frage gestellt. Während der Interviews wird auf Offenheit und Wertschätzung der Befragten geachtet, sodass beispielsweise aktive Unterbrechungen vermieden werden und bei Verständnisproblemen Nachfragen im Erfahrungs- und Verständniskontext des Befragten gestellt werden.[141] Außerdem wird versucht, die befragten Personen nicht durch gestellte Fragen in kausale Erklärungsnot und unter Druck zu setzen, womit womöglich verfälschte Antworten initiiert werden können. Dazu werden Fragen, welche auf eine kausallogische Antwort des Gegenübers abzielen, entsprechend umschrieben. Beispielsweise wird die Frage, warum eine neue Lösung eingeführt wurde, umformuliert in: „Wie kam es dazu, dass eine neue Lösung eingeführt wurde?" Diese Art der Fragestellung lässt der befragten Person mehr Offenheit in der Beantwortung und impliziert nicht zwingend eine rationale Antwort.

Abschließend wird darauf hingewiesen, dass alle Unternehmen für einen Teil oder die Gesamtheit ihrer Clients HP-Produkte einsetzen und der Forschende als Mitarbeiter der Firma HP auftritt. Möglicherweise leitet sich dadurch eine Beeinflussung oder eine bestimmte Erwartungshaltung der Expert*innen ab, welche jedoch nicht ausführlicher untersucht wird.

Vorliegende Datengrundlage

Als Datengrundlage dienen neun Experteninterviews mit verschiedenen Geschäftskunden der Firma HP. Mit den befragten Expert*innen wurde eine Erklärung zur Datenverarbeitung der erhobenen Daten vereinbart, welche in Anhang 2 zu finden ist und aus welcher hervorgeht, dass alle Daten lediglich anonymisiert verwendet werden. Da die Transkriptionen teils sehr

[138] Vgl. Pfadenhauer 2009, S. 453
[139] Pfadenhauer 2009, S. 453
[140] Vgl. Pfadenhauer 2009, S. 453 f.
[141] Vgl. Gläser/Laudel 2009, S. 48 ff.

detaillierte Aussagen enthalten, welche womöglich eine Identifizierung der Personen ermöglicht und, weil die Transkriptionen nicht derart anonymisierend und inhaltsverzerrend umgeschrieben werden sollen, werden die Transkriptionen mit einem Sperrvermerk versehen.

Mithilfe der Anonymisierung soll den Expert*innen Hemmungen genommen werden, welche auf die Identifizierung ihrer Person zurückzuführen sind. Außerdem gilt es festzuhalten, dass eine namentliche Kenntlichmachung der Personen keinem Zweck dieser Arbeit dienlich ist. Das Ziel von Experteninterviews ist die rekonstruierende Darstellung von Realumgebungen, welche in dieser Arbeit durch die Auswahlsituation und die Entscheidungsfindung von Client

Interviewtenkürzel	**Rollenbezeichnung**	**Dauer in Minuten**
IP1	Senior Workplace Architekt	38
IP2	Windows Basisinfrastruktur	30
IP3	Service Development BIOS und Treiber Management	25
IP4	Senior IT-Architect	34
IP5	Systemadministrator	26
IP6	Product Owner Basic Workplace Windows	24
IP7	Client Installation & HW Validation	54
IP8	Client Engineering Hardware Zertifizierung	40
IP9	WS Deployment Client Engineering	18

Tab. 2: Aufschlüsselung der Interviewpartner*innen, deren Positionen und die Dauer der Interviews.

Security Lösungen bestimmt werden.[142] Wie auch Abschnitt 3.2 zeigt, werden Personen als Experten*innen definiert, welche durch ihre berufliche Tätigkeit Einblicke in unternehmensinterne Beschaffungsvorgänge von Client Security Lösungen haben und die Faktoren dieser Vorgänge auf ihrer Erfahrung beruhend beschreiben können. Es wird versucht, möglichst viele Interviewpartner*innen zu gewinnen, welche eine aktive Rolle in der Beschaffung von Client Security Lösung einnehmen und Entscheidungskompetenzen innehaben. Wie aus Tabelle 2 zu entnehmen ist, sind exemplarische Rollenbezeichnungen der Expert*innen *Senior IT-Architect* (IP4), *Senior Workplace Architekt* (IP1) oder *Product Owner Basic Workplace Windows* (IP6). Interviewpartner IP6, IP7 und IP1 bis IP4 gestalten die Entscheidung, ob eine Client Security Lösung eingesetzt werden soll mit und können daher Erfahrungen aus erster Hand bei der Beantwortung der Fragen heranziehen. Die anderen Interviewpartner füllen Rollen aus, welche aus Perspektiven angrenzender Themenbereiche, wie der Hardwarezertifizierung, die Erfahrungsbeschreibungen mit Client Security Lösungen und deren Auswahl ermöglichen. Tabelle 3 liefert eine Möglichkeit, der für diese Arbeit charakteristischen Unternehmenseigenschaften der Expert*innen zu entnehmen. Befragt werden Expert*innen aus mittleren und großen Unternehmen, die meist (mit Ausnahme von IP2) für eine Anzahl von mehr als 100 000 Clients verantwortlich sind. Als Clients werden gemäß den Ausführungen der Forschungsfrage und der Ziele dieser Arbeit in Kapitel 1 diejenigen Endgeräte bezeichnet, welche windowsbetrie-

[142] Vgl. Gläser/Laudel 2009, S. 13

Interviewten-kürzel	Branche	Anzahl betreuter Clients	Anzahl MA
IP1	IT-Dienstleistung für Lebensmitteleinzelhandel	100 000	> 4 000
IP2	Banken und Finanzdienstleistungen	11 000	> 30 000
IP3	IT-Dienstleistung für Bundeswehr und Bund	160 000	> 5 000
IP4	IT-Dienstleistung für Bundeswehr und Bund	160 000	> 5 000
IP5	IT-Dienstleistung für Banken	160 000	> 6 500
IP6	IT-Dienstleistung für Verkehr und Logistik	111 100	> 5 100
IP7	IT-Dienstleistung	370 000	105 000
IP8	Telekommunikation	120 000	> 10 000
IP9	Telekommunikation	120 000	> 10 000

Tab. 3: Übersicht über die Unternehmen der befragten Personen.

bene Betriebsmittel der Unternehmen darstellen. Fünf der sieben befragten Unternehmen[143] sind IT-Dienstleister für einen oder wenige dedizierte Kunden, womit sich die hohe Anzahl der betreuten Clients im Vergleich zur geringen Mitarbeiterzahl erklären lässt. Zwei Unternehmen[144] bieten ihre IT-Dienstleistungen mehreren Kunden an, wobei sich die Angaben im Interview und die Anzahl der betreuten Clients von IP7 auf einen Kunden beziehen.

3.3 Qualitative Inhaltsanalyse als Methode der Datenauswertung

Aufgrund der relativ geringen Formalisierung der erhobenen Daten qualitativer Forschung wird in dieser Arbeit eine qualitative Inhaltsanalyse des Datenmaterials verwendet, um ein strukturiertes und stichhaltiges Verständnis der vorhandenen Interviewdaten zu ermöglichen.

Mayring unterscheidet drei verschiedene Grundformen der qualitativen Inhaltsanalyse, welche wiederum je mehrere Analysetechniken enthalten.[145] Die erste Grundform zielt auf eine *Zusammenfassung* der Daten ab, sodass „die wesentlichen erhalten bleiben“[146]. Diese Form kann durch induktive Abstraktion der Daten ein Modell als Ergebnis haben, welches die Daten reduziert abbildet. Als zweite Grundform wird die *Explikation* beschrieben, in welcher es verständnisschwierige Textstellen durch herangetragene Literatur zu erklären gilt.[147] Als abschließende Grundform wird die *Strukturierung* von qualitativen Datenmaterial genannt. Bei dieser Form werden bereits im Vorhinein definierte Ordnungskriterien, so genannte Kategorien, mit dem Material abgeglichen und anhand dessen werden deduktiv-geleitet Aussagen über

[143] Betrifft die Expert*innen IP1, IP2, IP3, IP4, IP6, IP8, IP9
[144] Betrifft Expert*innen IP5, IP7
[145] Mayring 2015, S. 67
[146] Mayring 2015, S. 67
[147] Vgl. Mayring 2015, S. 67 f.

die Daten ermöglicht.[148] In dieser Arbeit wird die deduktive Inhaltsanalyse nach Mayring angewandt, indem die in Kapitel 2.3 vorgestellten Dimensionen der ERP-Auswahl (Funktionalität, Anbieter, Interoperabilität, Kosten) als strukturierende Kategorien verwendet werden. Außerdem wird die in TAM definierte und auf die Akzeptanz einer nutzenden Person wirkende Determinante *wahrgenommene Benutzerfreundlichkeit* als zusätzliche Kategorie mitaufgenommen. Die zweite von Davis spezifizierte Hauptdeterminante *wahrgenommene Nützlichkeit* wird nicht explizit in das deduktive Kategoriensystem aufgenommen. Eine trennscharfe Unterscheidung zwischen der Dimension *Funktionalität* und der *wahrgenommenen Nützlichkeit* erscheint nicht möglich, da die Funktionalität aus der subjektiven Sicht der Befragten geschildert wird und damit deren Wahrnehmung der funktionalen Nützlichkeit enthalten kann. Dadurch erscheint eine differenzierte Unterteilung von subjektivem Empfinden der funktionalen Nützlichkeit und möglichst objektiver Betrachtung der Funktionalität im Rahmen dieser Forschung nicht durchführbar. In diesem Sinne wird in dieser Arbeit die Deckungsgleichheit in der Anwendung der Kategorie Funktionalität und die Analyse der *wahrgenommenen Nützlichkeit* unterstellt.

Darüber hinaus wird die Möglichkeit einer Erweiterung durch induktiv ermittelte Kategorien offengehalten. Die Expertenaussagen, die im Verlauf der dedukutiven Verfahrensweise, keiner übergeordneten Kategorie zugeordnet werden können, werden nach der schrittweisen Vorgehensweise nach Mayring paraphrasiert (Z1-Regel) generalsiert (Z2-Regel) und abschließend reduziert (Z3-Regel).[149]

3.4 Transkription

Als erster Schritt der Verarbeitung der erhobenen Daten werden die Aufnahmen der Interviews vollständig transkribiert. Da es in der empirischen Sozialforschung kein allgemeingültiges Regelwerk zur Transkription von Audioaufnahmen gibt, werden im Folgenden die in dieser Arbeit angewandten Regeln der Transkription erklärt.[150]

Die Festlegung auf den Detailgrad der Transkription und den Grad, in welcher das Interview abgebildet werden soll, hängt von der Forschungsfrage und dem Ziel der Untersuchung ab.[151] Detaillierte Transkriptionen dokumentieren auch nonverbale Ausdrücke wie Lachen oder Räuspern und paraverbale Äußerungen wie „hm“ oder „äh“.[152] Dieser Ansatz verfolgt eine möglichst vollständige Abbildung der aufgezeichneten Situation. Alternativ dazu reduziert eine gröbere Transkription, welche womöglich mit Korrekturen des Aufgezeichneten versucht die Lesbarkeit zu erhöhen, unweigerlich den Informationsgehalt des Datenmaterials.[153]

[148] Vgl. Mayring 2015, S. 67 f.
[149] Vgl. Hussy/Schreier/Echterhoff 2010, S. 34 ff.
[150] Vgl. Petra Suwalski 2020, S. 121
[151] Vgl. Gläser/Laudel 2009, S. 193 f.
[152] Vgl. Gläser/Laudel 2009, S. 193 f.
[153] Vgl. Dresing/Pehl 2020, S. 843 f.

In dieser Arbeit wird kein Erkenntnisgewinn aus einer feingranularen Transkription erwartet, sodass eine einfache, glättende Transkription für eine bessere Lesbarkeit mit den folgenden Regeln als Verfahren festgelegt wird:

- Umgangssprachliche und dialektische Redewendungen wurden, wo es denn möglich war, in einen hochdeutschen Ausdruck überführt.
- Satzabbrüche und kontextschwierige wechselnde Gedankensprünge wurden durch möglichst wenige Anpassungen in eine sprachlogische Form gebracht.
- Wortdopplungen und Versprecher wurden nicht in das Transkript aufgenommen.
- Satzzeichen wurden entsprechend der Orthographie gesetzt und in Ausnahmefällen durch die Sprachmelodie geleitet.[154]
- Personennamen wurden aufgrund der Wahrung der Anonymität der Studienteilnehmer entfernt und durch bezeichnende Platzhalter ersetzt.[155]
- Alle von den genannten Regeln nicht berührten verbalen Äußerungen wurden vollständig transkribiert, wobei keine inhaltslogische Formatierung, beispielsweise durch Absätze, vollzogen wurde.

3.5 Kodierleitfaden und Definitionen

Wie in Kapitel 3.3 beschrieben, wird eine deduktiv strukturierende Inhaltsanalyse nach Mayring durchgeführt. Dafür werden aus den Transkriptionen der Experteninterviews gewichtig erscheinende Paraphrasen zur Beantwortung der Forschungsfrage extrahiert. Diese Paraphrasen werden anschließend den deduktiven Kategorien *Kosten*, *Funktionalität*, *Interoperabilität*, *Anbieter* und *Benutzerfreundlichkeit* zugeordnet.

Kategorie	**Definition**
Kosten	Beschreibt monetäre Aufwendungen, für Anschaffung oder Betrieb einer Client Security Lösung
Funktionalität	Beschreibt Zweck und Nutzenstiftung einer Client Security Lösung
Interoperabilität	Beschreibt Integrationsmöglichkeiten und Schnittstellen zur Datenübertragung
Anbieter	Beschreibt charakterisitische Eigenschaften eines Anbieters
Benutzerfreundlichkeit	Beschreibt Eigenschaften einer Client Security Lösung, welche die Benutzung erleichern

Tab. 4: Definition der Kategorien zur deduktiven Anwendung.

[154] Vgl. Dresing/Pehl 2020, S. 846
[155] Vgl. Gläser/Laudel 2009, S. 194

Diese Zuordnung erfolgt anhand der in Tabelle 4 dargestellten Kategorien, wobei ein detaillierter Kodierleitfaden in Anhang 4 zu finden ist. Zuerst wird für alle Paraphrasen geprüft, ob sie einer der Definitionen der Kategorien entsprechen. Falls anhand der Definitionen keine eindeutige Zuordnung erfolgen kann, wird im zweiten Schritt getestet, ob sich die Paraphrase mittels einer der Kodierregeln zuordnen lässt. Es ist also wichtig, dass das Kategoriensystem die einzelnen Kategorien klar definiert, um eine zweifelsfreie Einteilung zu ermöglichen. Da einzelne Paraphrasen mehrere Kategorien thematisieren können ist eine mehrfache Zuteilung zu verschiedenen Kategorien möglich.

4 Auswahlkriterien von Client Security Lösungen

Zielsetzung: Dieses Kapitel widmet sich der erschließenden Darstellung der empirischen Forschungsergebnisse, welche aus der Durchführung der im vorherigen Kapitel erläuterten Forschungsmethode der Experteninterviews hervorgegangen sind. Mithilfe der folgenden Ausführungen der Ergebnisse soll der Beantwortung der Forschungsfrage durch eine analytisch-diskutierende Darlegung möglich werden. Abschließendes Ziel dieses Kapitels ist es, ein abstrahierend-zusammenfassendes Modell vorzustellen, welches die Auswahlkriterien der Client Security Lösungen in Bezug zueinander setzt. Dieser Teil bildet damit den Abschluss des in Kapitel 3.1 beschriebenen Forschungsdesigns.

Aufbau: Zunächst führt dieses Kapitel die Überlegungen des vorherigen Kapitels bezüglich der Auswertung der erhobenen Daten fort und legt die Auswertung der Experteninterviews, strukturiert in Unterkapiteln je herangetragener Kategorie, offen. Pro Kategorie erfolgt als erstes eine neutrale Beschreibung der Erkenntnisse, die auf Basis der Inhaltsanalyse erzielt werden konnten. Als zweites werden die Beobachtungen interpretativ diskutiert und hinsichtlich der Beantwortung der Forschungsfrage eingeordnet. Die Interpretationen der einzelnen Kategorien werden im letzten Unterpunkt zusammengetragen und in einem Verständnismodell manifestiert.

4.1 Funktionalität

Wie bereits aus den Ausführungen in Kapitel 2.3 hervorgeht, bestimmt die Funktionalität einer Lösung den Anwendungszweck und damit mögliche Einsatzfelder. Den übergeordneten Zweck der Client Security Lösungen beschreibt IP1 äußerst trivial:

> *Vertrauen ist gut und so. Aber manchmal ist halt die Kontrolle doch besser.*

Dieser Anspruch nach Kontrolle zieht sich über die im Folgenden aufgeführten Kriterien hinweg und drückt sich beispiellos in der Verlässlichkeit der Lösung aus. Ist das Verhalten der Lösung transparent und erfüllt die ursprünglichen Erwartungen, so wird die Lösung als verlässlich wahrgenommen.[156] Im Client Security Kontext setzen Teile der Expert*innen diese Kontrolle mit der Sicherheit und Limitation der Anwenderfreiheiten gleich. [157]

Als ein wichtiger Mechanismus der funktionalen Sicherheit wird der Einsatz eines präzisen Rechtemanagements von vielen Expert*innen für den Schutz auf der Ebene des Betriebssystems eines Clients betrachtet. Es wird angeführt, dass das Rechtemanagement die Umsetzung und das Verwalten einer spezifischen Zugangskontrolle ermöglicht, welche insbesondere die Fernverwaltung der Clients unterstützt.[158] Dementsprechend ergeben die Aussagen

[156] Vgl. IP 2021
[157] Vgl. IP2 2021, Vgl. IP7 2021
[158] Vgl. IP2 2021

der Expert*innen, dass sechs der sieben Unternehmen den Anwender*innen keine vollumfänglichen Rechte auf den genutzten Clients gewähren und sicherheitskritische Einstellungen durch die zentrale Administration vorgegeben werden.[159] Mithilfe dieser Maßnahme soll einerseits verhindert werden, dass die Anwender*innen eventuelle Bedrohungen durch beispielsweise schädliche Installationen von Applikationen ermöglichen.[160] Andererseits stellt diese Umsetzung des Rechtemanagements sicher, dass alle Clients einheitlich konfiguriert werden können und damit Sicherheitsanforderungen formalisiert umgesetzt werden.[161] Die einheitlichen Eigenschaften der Clients unterstützen wiederum eine präzisere Einschätzung über das System- und Client-Verhalten, sodass mögliche Fehlerursachen auf das einheitliche Verhalten limitiert werden können und berechenbarer werden.[162] Auf diesem Rechtemanagement aufbauend wird als Kriterium für die Funktionalität einer Client Security Lösung die Remote-Steuerung, also die Fernsteuerung eines Clients, der Lösungen auf dem Client benannt. Wird diese Remote-Steuerung durch Automation im Management der Lösungen ergänzt, fällt nach Aussagen der Expert*innen weniger Arbeit für die Administratoren der Lösungen an.[163] Die Automatisierung von Arbeitsschritten muss auch dahingehend positiv bewertet werden, dass individuelle menschliche Fehler vermieden werden und ein standardisiertes Ausführen der bestimmten Arbeitsschritte gewährleistet wird.[164] IP1 fasst die genannten Aspekte folgendermaßen zusammen:

> *Deshalb dürfen die Anwender nix selbst installieren und wir können aber auf der anderen Seite natürlich auch automatisiert Software ausbringen.*[165]

Mit dem Rechtemanagement und einer autorisierten Zugangskontrolle geht die Thematik des Passwortes, welches klassischer Weise die Authentifizierung eines Nutzenden gewährleistet, einher. Von Teilen der Interviewpartner*innen wird diesbezüglich eine Abschaffung vorhandener Passwort-Mechanismen gefordert und der Einsatz von „passwort-less“[166] Verfahren angestrebt. Nachteilig ist hierbei die mögliche Weitergabe des Passworts:

> *Und dann haben wir die Erfahrung gemacht, dass sich das praktisch wie ein Lauffeuer verbreitet hat.*[167]

Außerdem erweisen sich Passwörter im Kontext des autorisierten BIOS-Zugriffs als Herausforderung im Management, was nach Angaben der Expert*innen dazu führt, dass kaum clientspezifische Passwörter benutzt werden und sie nur selten geändert werden.[168] Als Alternative

[159] Vgl. IP1 2021, Vgl. IP2 2021, Vgl. IP3 2021, Vgl. IP5 2021, Vgl. IP7 2021, Vgl. IP8 2021
[160] Vgl. IP7 2021
[161] Vgl. IP1 2021
[162] Vgl. IP7 2021
[163] Vgl. IP1 2021, Vgl. IP4 2021, Vgl. IP6 2021
[164] Vgl. IP1 2021
[165] IP1 2021, Z. 152 f.
[166] Vgl. IP6 2021, Z. 190
[167] Vgl. IP8 2021, Z. 176 f.
[168] Vgl. IP1 2021, Vgl. IP2 2021, Vgl. IP6 2021

zu einem Passwort-Schutz werden Mechanismen genannt, welche mit der Verwendung von digitalen Zertifikaten[169] arbeiten.[170] Die Zertifikate werden aufgrund der kryptografischen Verschlüsselung eine unautorisierte Manipulation und Fälschung der Zugangsdaten erschweren. Dies führe zu einem höheren Sicherheitsniveau, in welchem niemand „ein Kennwort kennen muss“[171].

Unterliegen die Unternehmen bestimmten gesetzlichen Vorgaben, so kann es notwendig sein, dass die Client Security Lösungen gewisse Zertifizierungen oder Standards erfüllen müssen.[172] Dabei indizieren Zertifizierungen bestimmte Qualitätsmerkmale, welche oft mit den Eigenschaften des Anbieters korrelieren beziehungsweise für den Anbieter ausgestellt werden. Dahingehend besteht eine enge Verknüpfung zwischen den Sicherheitsanforderungen an eine Client Security Lösung und den Sicherheitsanforderungen an einen Anbieter.

In Bezug auf die notwendige Verbreitung des BIOS-Passworts, um „Support, Installierbarkeit und Management“[173] zu ermöglichen, stellt sich heraus, dass nicht angestrebt wird, das Domänenwissen der Sicherheitsmechanismen jedem zugänglich zu machen. Es wird also beabsichtigt einige wenige Spezialisten für die Verwaltung der BIOS-Sicherheit einzusetzen.

Als Teil der funktionalen Anforderungen an Client Security Lösungen wird eine möglichst große Plattformunabhängigkeit genannt, welche in Summe aller Clients zu einer möglichst geringen Anzahl an zu betreibenden Lösungen führt.[174] Diese Plattformunabhängigkeit, so führen die Expert*innen fort, sei umso vorteilhafter, je größer die Anzahl an betreuten Clients ist.[175] Aus der Menge der betreuten Clients leitet sich auch eine Forderung nach skalierbaren Eigenschaften der Client Security Lösung ab, welche sich durch Automation, Remote-Management und Verlässlichkeit des Systems manifestieren kann.[176]

Als ein funktionales Qualitätsmerkmal von Client Security Lösungen gelten die Verlässlichkeit, Aktualität und Verfügbarkeit einer Lösung.[177] Je nach Einsatzgebiets und der Art des Schutzes müssen diese Merkmale unterschiedlich gewichtet betrachtet werden. Beispielsweise sind bei einer Antivirenlösung die Aktualität und ständige Verfügbarkeit der Lösung essenziell. Gezielt wird dabei auf die verpflichtende Eigenschaften abgezielt, die einen sicheren Betrieb der Clients gegenüber dynamischer Bedrohungspotentiale durch die Überwachung der Lösung gewährleisten soll.[178] Im Gegenzug gibt es Client Security Lösung, die reaktiv und nicht ständig verfügbar sein müssen. Exemplarisch sind an dieser Stelle Mechanismen der Festplattenverschlüsselung genannt, die vor Betriebssystemstart des Clients eine Prüfung auf veränderte

[169] Digitale Zertifikate dienen der autorisierten Zugangskontrolle und werden zur Identifikation autorisierter Zugriffe genutzt. Sie bauen auf kryptografischen Verfahren wie der asymmetrischen Verschlüsselung auf.
[170] Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP7 2021, Vgl. IP8 2021
[171] Vgl. IP4 2021, Z. 53
[172] Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP6 2021
[173] Vgl. IP4 2021, Z.49
[174] Vgl. IP8 2021, Vgl. IP4 2021
[175] Vgl. IP8 2021, Vgl. IP4 2021
[176] Vgl. IP4 2021, Vgl. IP7 2021
[177] Vgl. IP1 2021, Vgl. IP2 2021, Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP6 2021
[178] Vgl. IP7 2021, Vgl. IP9 2021

Hardwarekomponenten vornehmen und eine entsprechende Zugangsberechtigung durchführen, um den Datenzugriff zu autorisieren oder abzulehnen.

Abschließend bleibt festzuhalten, dass je nach verfolgtem Schutzziel entsprechend spezifische Funktionalitätsanforderungen an die Client Security Lösungen gestellt werden.[179] Diese spezifischen Kriterien werden durch die folgenden, allgemeinen funktionalen Kriterien für Client Security Lösungen umrahmt:

- Autorisierung von Einstellungsmöglichkeiten der Lösung nur für bestimmte Berechtigungsgruppen.
- Remote-Management für das Verwalten, Kontrollieren und Einstellen der Lösungseigenschaften.
- Managementansätze, welche die skalierbare Verwaltung der Lösung ermöglichen.
- Allgemeine Automatisierungsmöglichkeiten der Lösung.
- Verfügbarkeit und Verlässlichkeit der Lösung.

4.2 Interoperabilität

Die Interoperabilität wird durch Standards und andere Formalisierungen erhöht, sodass verschiedene Anwendungen und Systeme über festgelegte Schnittstellen und Protokolle miteinander interagieren können. Zur Umsetzung dieser Standards, wird eine Forderung nach Standardlösungen genannt, welche sich durch standardisierte Eigenschaften auszeichnet. So beschreibt eine befragte Person die Strategie des eigenen Unternehmens hinsichtlich der Systemarchitekturen dahingehend, dass die Architektur den Einsatz von Standardlösungen ermöglichen solle.[180] Daraus ergibt sich eine Bereitschaft des Unternehmens, die eigene Architektur anzupassen, falls keine Standardlösung in die bisherige Struktur implementiert werden kann. Anspruch ist es dabei, das einzuführende Produkt „möglichst unverändert“[181] zu belassen.

Ein wichtiger Faktor der Interoperabilität ist die Datenübertragung zwischen verschiedenen Systemen und Anwendungen. Dieser Datenaustausch kann bei bestimmten Client Security Lösungen für die Dokumentation von Ereignissen, wie der Feststellung einer Sicherheitsbedrohung, wichtig sein.[182]

Außerdem wird die Interoperabilität oft in Ansätzen der Automation einer Lösung relevant, wenn die automatische Steuerung nicht von der Client Security Lösung selbst, sondern von

[179] Vgl. IP6 2021
[180] Vgl. IP6 2021
[181] Vgl. IP6 2021, Z. 162
[182] Vgl. IP2 2021

einem verwaltenden Programm getätigt wird. Derlei Automatismen werden häufig über Konsolenschnittstellen und spezifische Befehle ermöglicht. Dieser Ansatz der Automation ermöglicht folglich auch die Berücksichtigung von Managementaspekten.

Eine schlechte Interoperabilität kann sich negativ auf die Leistung der Nutzer*innen auswirken, da sich verschiedene Lösungen sich in ihrer Funktionalität nicht ergänzen, sondern vielmehr blockieren.

Keine der befragten Personen hat Veränderungen der Systemarchitektur kategorisch ausgeschlossen, sondern auf die Beachtung des „Kosten-Nutzen-Faktors“[183] verwiesen. Wichtig sei allerdings, dass die Anpassung der internen Systeme keinen regelmäßigen Charakter habe:

> *Aber ich darf nicht gezwungen sein, weil der Hersteller jede Woche so ungefähr sein Konzept ändert, jede Woche meine Architektur anpassen zu müssen.*[184]

Die Interoperabilität ist ein kritischer Faktor für das erwartungsgemäße Funktionieren einer Client Security Lösung, da mit der Menge an verschiedenen Lösungen und deren Schnittstellen die Vernetzung und damit die Interdependenzen der Lösungen untereinander steigen. Die Änderung einer Lösung kann somit viele Veränderungen an anderen Stellen nach sich ziehen, damit die Systemfunktionalität bestehen bleibt. Dadurch können Resistenzen bei den Anwender*innen entstehen,[185] die eine Veränderung einer Lösung, beispielsweise durch ein Update, als potentiellen Grund für Fehler im Systemverhalten sehen.[186]

Eine Möglichkeit eine Lösung anbieten zu können, die in verschiedenen Systemen ohne deren Anpassung implementiert werden kann, stellen Konfigurationseinstellungen der Lösung dar. Dies kann mit dem folgenden Anspruch zusammengefasst werden:

> *Wir wollen Standardlösungen von renommierten Herstellern, also von den Top-Anbietern, die dann entsprechende Konfigurationsmöglichkeiten bereits mitbringen.*

Eine spezielle Rolle kommt der Interoperabilität den Client Security Lösungen dadurch zu, dass bestimmte Client Security Lösungen den Zugriff und das Verhalten anderer Lösungen kontrollieren. Diese Art der Client Security Lösungen steuern also aktiv die Interaktion von anderen Lösungen und kontrollieren in diesem Maße die Sicherheit. Eine befragte Person erläutert, dass eine im Unternehmen betriebene Lösung nach vorliegenden Sicherheitsbedrohungen auf einem Client sucht und im Bedarfsfall sperrt die Lösung „den Zugriff auf interne Unternehmensressourcen beispielsweise ab“[187].[188] Abschließend kann festgehalten werden, dass die Interoperabilität durch folgende Faktoren beeinfluss werden kann:

[183] Vgl. IP3 2021, Z. 163
[184] Vgl. IP9 2021, Z. 107 f.
[185] Vgl. Abschnitt 2.2
[186] Vgl. IP6 2021
[187] Vgl. IP6 2021, Z. 178
[188] Siehe dazu auch: Vgl. IP1 2021

- Interaktions- und Datenaustauschmöglichkeiten durch standardisierte Schnittstellen und Protokolle.
- Zugriff auf Steuerungsprozesse der Lösung.
- Vernetzung und Kompatibilität der Lösung mit der existierenden Umgebung.

4.3 Kosten

Die Kosten von Client Security Lösungen lassen sich nach den Angaben der Befragten in Planungs-, Test-, Implementierungs- und Betriebskosten einteilen.[189] Während die Kosten für Planungen und Testungen vor der eigentlichen Auswahl auf eine Lösung anfallen, entstehen die Implementierungs- und Betriebskosten erst nach der Festlegung auf eine bestimmte Client Security Lösung. Die erstgenannten Kosten scheinen dabei die weiteren Kosten in dem Maße zu bedingen, dass mit einer geschickten Auswahl und Anpassung der Lösung, möglichst wenige Folgeaufwände im Betrieb durch Abänderungen, Fehlerbehebung oder Support entstehen.[190]

Mit steigender Anzahl an Clients erhöht sich die Gewichtigkeit, Automatismen im Betrieb der Lösungen einzusetzen und damit an Personalkosten sparen zu können. Diese Automatismen müssen im Vorhinein geplant und getestet werden:

> *Das muss verlässlich und automatisch alles möglichst ablaufen. Deshalb haben wir ja umfangreiche Testdurchläufe und Evaluierungsdurchläufe im Vorfeld, denn danach muss es einfach funktionieren. Also wir haben weder Ressourcen nachher oder andere Möglichkeiten, das irgendwie anderweitig zu berichtigen. Also wenn irgendwo ein Fehler ist oder wenn das nicht zuverlässig funktioniert, könnten wir einfach gar nicht das Ganze auf anderen Wegen geradebiegen.*[191]

Das Zitat zeigt dabei auch den limitierenden Charakter der Kosten auf, sodass manche händischen Eingriffe mittlerweile unmöglich erscheinen. Demzufolge sind die Unternehmen der befragten Expert*innen bereit, in lange Testphasen zu investieren, um das zukünftige Funktionieren der Lösung gewährleisten zu können.

Eine Besonderheit zeigt sich bei den Unternehmen, welche den Bedarf einer Security Lösung ausschreiben. Diese Unternehmen definieren einen detaillierten Anforderungskatalog, sodass bei Erfüllen dieser Anforderungen „die kostengünstigste Lösung den Zuschlag“[192] erhält. Bei

[189] Vgl. IP4 2021, Vgl. IP6 2021
[190] Vgl. IP4 2021
[191] Vgl. IP4 2021, Z. 64-70
[192] Vgl. IP6 2021, Z. 60 f.

Ausschreibungen, welche sehr hohe Sicherheitsanforderungen definieren, kann es jedoch vorkommen, dass nur eine spezifische Lösung die Anforderungen erfüllt und damit eine Auswahl entfällt.[193]

Als weiterer Kostenfaktor wurden Lizenzkosten genannt, welche während des Betriebs und meistens pro Client berechnet werden.[194] Daher „summiert sich dann halt dementsprechend [jeder Euro]“[195], der für eine Clientlizenz anfällt und kann damit einen entscheidenden Faktor bei der Auswahl einer Client Security Lösung darstellen.

Alle Expert*innen gaben an, dass eine getroffene Auswahl für eine bestimmte Client Security Lösung für mehrere Jahre gilt und an der Client Security Lösung möglichst lange festgehalten werden soll, damit sich die anfänglichen hohen Kosten in Testung und Implementierung als lohnenswert herausstellen können. Eine Ausnahme hierbei stellen Unternehmen dar, welche aufgrund gesetzlicher Rahmenbedingungen, regelmäßig Ausschreibungen platzieren müssen und daher gezwungen werden, neue Lösungen in Betracht zu ziehen müssen. Jedoch werden die Ausschreibungen meist auch auf mehrere Jahre festgesetzt.[196]

Zusammenfassend lässt sich folgendes festhalten:

- Die Kosten limitieren die infrage kommenden Client Security Lösungen.
- Die Bedeutung von Lizenzkosten steigt mit der Zunahme der Anzahl an betreuten Clients.
- Um die Funktionalität im Betrieb sicherstellen zu können und die Möglichkeiten unberechenbarer Folgekosten zu limitieren, werden aufwändige Testphasen durchgeführt.

4.4 Anbieter

Der Anbieter und seine angebotenen Leistungen werden von den Interviewpartner*innen in starken wechselseitigen Zusammenhang gesehen, sodass die Wahl auf einen qualitativen Anbieter als Platzhalterentscheidung für die Auswahl einer qualitativen Lösung getroffen wird. Dieser Mechanismus beinhaltet auch die Forderungen an einen Anbieter, sich verlässlich, transparent und konsistent zu verhalten, um damit eine entsprechende Qualität der Lösung erwarten zu können.[197]
Beispielhaft für diesen Zusammenhang berichtet eine befragte Person von dem Verkauf eines Client Security Anbieters an einen Dritten. Dieser Verkauf stellte für das Unternehmen der befragten Person einen Grund dar, den neuen Anbieter überprüfend zu bewerten und davon

[193] Vgl. IP3 2021, Vgl. IP4 2021
[194] Vgl. IP1 2021, Vgl. IP2 2021, Vgl. IP7 2021
[195] Vgl. IP1 2021, Z. 136
[196] Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP6 2021
[197] Vgl. IP4 2021

abhängig zu entscheiden, ob die Lösung weiterhin genutzt werden soll - gleichwohl die eingesetzte Lösung[198] in ihren weiteren Rahmenbedingungen nicht verändert wurde.[199]

Gleichzeitig unterstreichen die Interviewteilnehmer*innen, dass die Anschaffung einer Client Security Lösung für einige Jahre getroffen wird. Teilweise wurden die Auswirkungen der Entscheidungen auf fünf oder mehr Jahre angesetzt, wobei eine*r der Interviewpartner*innen berichtet, dass eine Antivirenlösung desselben Anbieters fünfzehn Jahre lang eingesetzt wurde.[200] Diese langfristig angestrebte Nutzung einer Security Lösung liegt auch in den hohen Planungs-, Testungs- und Implementierungsaufwände begründet.[201]

Die Größe des Unternehmens, bisherige Referenzen und andere Reputationen attestieren dem Anbieter Kompetenz in der Domäne der Client Security.[202] Aus der Größe des Unternehmens wird die Fähigkeit abgeleitet, die Kund*innen durch einen schnellen, ausführlichen und konstruktiven Service und Support zu unterstützen, welche mit steigender Anzahl der betreuten Clients[203] und der Komplexität der eigenen Systeme[204] an Wichtigkeit zunimmt. Die unterstützende Interaktion des Anbieters wird mit einem hohen Stellenwert beurteilt, was die folgende Aussage unterstreicht:

> *(Es ist wichtig, dass der Anbiter) in regelmäßigen Abständen dementsprechend Updates anbietet [. . .] und da müssen natürlich die Security-Firmen dann permanent aktiv sein.* [205]

Der Anspruch einer langfristigen Nutzung der Client Security Lösung und die Forderung nach „Aktivität“ der Anbieter deuten darauf hin, dass eher ein Anbieter ausgewählt wird als eine spezifische Lösung.

Zwei Interviewpartner*innen gaben an, dass sich die Sicherheitsanforderungen an die Client Security Lösungen aus gesetzlichen Grundlagen ergeben würden. Demzufolge setzen diese Unternehmen eine Erfüllung der Vorlagen durch den Anbieter und teils auch Zertifizierungen des Anbieters voraus, welche sich in den genannten Fällen aus den Anforderungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Sektorenordnung für Verkehrsunternehmen.[206] Das führt dazu, dass das eigene Unternehmen „nicht irgendeinen Nischenanbieter“ auswählen könne und auf Grundlage der Sektorenverordnung regelmäßig Ausschreibungen aufstellen muss.[207]

[198] In dem angeführten Beispiel wurden sämtliche Leistungen und bestehenden Verträge durch den neuen Eigentümer fortgeführt.
[199] Vgl. IP2 2021
[200] Vgl. IP9 2021
[201] Vgl. IP2 2021
[202] Vgl. IP2 2021, Vgl. IP6 2021, Vgl. IP4 2021
[203] Vgl. IP1 2021, Vgl. IP4 2021, Vgl. IP6 2021
[204] Vgl. IP4 2021
[205] IP7 2021, Z. 514-517
[206] Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP6 2021
[207] Vgl. IP6 2021

Diese These stellt die Frage auf, inwiefern und ob überhaupt Innovationen von den Kund*innen erwünscht werden. Den Ausführungen der Expert*innen zufolge müssen innovative Lösungen mangels Referenzen prinzipiell skeptisch betrachtet werden und werden eher als ungeeignet bewertet. Für einen Anbieter kann dies bedeuten, dass lediglich granulare Innovationen in bereits vorhandene Lösungen implementiert werden und damit ein fortlaufendes Erneuern der Lösungen umgesetzt wird.

Da aus den Eigenschaften eines geeigneten Anbieters die Qualitätsurteile dessen Lösungen abgeleitet werden, scheint die Dimension des Anbieters auf alle Arten von Client Security Lösungen eine wichtige Rolle einzunehmen. Insbesondere die Größe der in dieser Forschungsarbeit untersuchten Unternehmen prägt die Auswahl von Client Security Lösungen in der Weise, dass mit unbedingtem Willen die „richtige“ Enscheidung getroffen wird, in dem Sinne, dass die Lösung des Anbieters im erwarteten Maße funktioniert und entsprechend lange an der Lösung festgehalten werden kann, sodass sich die Aufwendungen in Auswahl, Planung und Implementierung gelohnt haben. Integrität und Langfristigkeit ausführen.

Bei der Auswahl des Anbieters spielen auch Sorgen hinsichtlich möglicher Ausfälle eine tragende Rolle. So sind die Kunden darauf bedacht, einen Anbieter auszuwählen, der möglichst ständig für Unterstützung und Beratung zur Seite steht und seine Produkte entsprechend gestaltet, dass diese keine Ausfälle nach sich ziehen. Andererseits prägt die Auswahl auch das Worst-Case-Szenario, dass die eingesetzte Lösung auf den betriebenen Clients zu Ausfällen der Funktionalität der Lösung oder zu ganzen Systemausfällen führt. Vor diesem Hintergrund wird mit steigender Anzahl an Clients ein höherer Druck auf die Auswahl einer Lösung beschrieben. [208] Es bleibt zusammenfassend festzuhalten, dass die folgenden Kriterien einen Anbieter auszeichnen:

- Bisherige Referenzen unterstreichen die Kompetenzen des Anbieters.
- Die Größe des Anbieters
- Die Vertrauenswürdigkeit kann durch Zertifizierungen und das Erfüllen von Standards bestätigt werden.
- Die Marktpositionierung des Anbieters bestätigt bisherige Erfolge.
- Reputation

4.5 Benutzerfreundlichkeit

Die Benutzerfreundlichkeit kann im Kontext der Client Security Lösungen hinsichtlich zwei verschiedener Gruppen von Benutzer*innen untersucht werden. Einerseits kann sich die Lösung als benutzerfreundlich gegenüber den Anwender*innen der Clients äußern. Andererseits

[208] Vgl. IP1 2021, Vgl. IP2 2021, Vgl. IP3 2021, Vgl. IP8 2021

werden die Client Security Lösungen in Unternehmen meist von Administratoren verwaltet, welche sich in ihrer alltäglichen Arbeit mit der zentralen Organisation und Kontrolle der Lösungen beschäftigen.[209]

Die Benutzerfreundlichkeit einer Client Security Lösung zeichnet sich gegenüber der Anwender*innen darin aus, dass es „die beste Lösung ist es, wenn der Enduser das gar nicht merkt, wenn die im Hintergrund arbeitet“[210]. Ein andere befragte Person führt den Anspruch fort, „dass sie [Client Security Lösungen] sich sehr gut selbst verstecken“[211] können und weder durch Anwender*innen gesteuert noch bemerkt werden sollen. Hinsichtlich des laufenden Betriebs muss man zwischen Client Security Lösungen differenzieren, welche im ständigen Betrieb aktiv sein müssen, wie beispielsweise Antivirenlösungen, welche jederzeit mögliche Sicherheitsrisiken feststellen sollen. Neben solchen Lösungen gibt es weitere, die erst durch eine spezifische Aktion initiiert und erst zu diesem Zeitpunkt aktiviert werden. Zu diesen Lösungen gehören beispielsweise Festplattenverschlüsselungen, welche beim Start des Clients aktiv nach möglichen Manipulationen suchen. Die erstgenannte Art der Client Security Lösungen ist daher besonders anfällig für den Verbrauch von Systemressourcen, welche den Anwender*innen nicht mehr zur Verfügung stehen und nicht dazu führen, dass „der Anwender vernünftig arbeiten kann“[212].

Für Administratoren hingegen indizieren Übersichtlichkeit, Möglichkeiten der Automation, intuitiver Aufbau und Handhabung eine Benutzerfreundlichkeit der Client Security Lösungen.[213] In Bezug auf die Implementierung und Weiterentwicklung der eigenen System werden Lösungen als positiv bewertet, welche man aufgrund ihres Aufbaus „schnell testen kann“[214] und daher auch schnell in ihrer Nutzung erlernbar sind. IP4 führt dazu weiter aus, dass eine entsprechende Unterstützung der Bedienung durch geeignete Dokumentationen des Anbieters erfolgen kann.[215]

Automation spielt an dieser Stelle ebenfalls eine funktionale Rolle, da somit eine performantere Funktionsfähigkeit der Lösung erreicht werden kann, was wiederum als positiv von den Nutzer*innen während der Bedienung des Systems empfunden wird. Zusammenfassend nehmen folgende Aspekte auf die Benutzerfreundlichkeit Einfluss:

- Strukturierte Dokumentationen des Admins zur Nachvollziehbarkeit für Nutzer*innen.
- Klares und vereinfachtes Zugriffs- und Rechtemanagement für Admin.
- Vielfältige Bedien- und Anpassungsmöglichkeiten für Admin ermöglichen.

[209] Vgl. IP1 2021, Vgl. IP3 2021, Vgl. IP6 2021
[210] Vgl. IP1 2021, 320 f.
[211] Vgl. IP2 2021, Z. 166 f.
[212] Vgl. IP9 2021, Z. 60
[213] Vgl. IP2 2021, Vgl. IP4 2021, Vgl. IP6 2021
[214] Vgl. IP8 2021, Z. 255 f.
[215] Vgl. IP4 2021

Die zusätzlichen Nutzenden des Systems scheinen hinsichtlich der genannten Faktoren nur geringfügigen Einfluss zu nehmen.

4.6 Service und Support

Im Verlauf der Zuordnung wurde festgestellt, dass einige Paraphrasen keiner der vorab festgelegten Auswahlkriterien[216] zugeordnet werden konnten. Diese verbliebenen Paraphrasen wurden nach der induktiven Inhaltsanalyse von Mayring zunächst generalisiert und dann auf Kernaussagen reduziert. Durch dieses Verfahren entstand eine sechste Kategorie: Service und Support. Das detaillierte Vorgehen der Kategorienbildung kann in Anhang 6 nachvollzogen werden.

Die Interviewpartner*innen führen die Unterstützung des Anbieters bei Implementierung und Fehlerbehebung der Client Security Lösung als ein wichtiges Kriterium der Auswahl an. Beispielsweise kann eine mangelnde Unterstützung des Anbieters bei der Fehlerbehebung einer Lösung dazu führen, dass der Anbieter in zukünftigen Ausschreibungen nicht mehr berücksichtigt wird.[217] Bei einigen Subklassen von Client Security Lösungen sind die Aktualität der Lösungen, welche mittels Updates sichergestellt werden, für die Funktionalität der Lösungen und der Bewahrung des Sicherheitsanspruchs entscheidend. Dies ist beispielsweise bei Antivirenlösungen der Fall, da diese unmittelbar auf neue Viren und andere Bedrohungen reagieren müssen, um die stetige Sicherheit des Clients zu gewähr.[218] Die Updatehäufigkeit und das erfolgreiche implementieren dieser Updates stellen somit einen Kern der Antivirenlösungen dar, welcher bei einer mangelhaften Umsetzung und Problemen in der Aktualität zu Einbußen in der Funktionalität (kein aktueller Virenschutz vorhanden) und Aufwänden in der Fehlerbehebung der Unternehmen führen kann.[219] Mit der Thematik der Updates und der regelmäßigen Aktualisierung der Client Security Lösungen verbindet sich auch der Ansatz der befragten Unternehmen, selten die Lösungen austauschen zu müssen. In diesem Verständnis bildet das Aktualisieren einen eigenen funktionalen Anspruch ab, welcher sich mit der Erwartung verbindet, dass der Anbieter „permanent aktiv“[220] ist und bei Bedarf „schnellstmöglich eine Lösung parat stellt“[221]. Ein Spezialfall stellt das BIOS-Update dar. Das BIOS kann mittels eines Passworts vor unautorisierten Zugriffen und Manipulationen geschützt werden. Falls ein solcher Zugriffsschutz aktiv ist, so muss das Passwort bei der Durchführung eines Updates zur Authentifizierung angegeben werden. Updates verändern die Software von Lösungen und führen dadurch zu einem anderen Verhalten der Software. Daher müssen Updates wie auch andere Datenzugriffe und -veränderungen möglichst sicher gestaltet werden. Der Updatemechanismus an sich kann also als Gegenstand der Sicherheit verstanden werden. Gerade Updates

[216] Vgl. Abschnitt 4.1-4.5
[217] Vgl. IP8 2021
[218] Vgl. IP9 2021, Vgl. IP8 2021, Vgl. IP2 2021
[219] Vgl. IP9 2021
[220] Vgl. IP7 2021, Z. 517
[221] Vgl. IP7 2021, Z. 520

zu Konfigurationseinstellungen, da nicht alle Updates der Anbieter auf den Clients installiert werden sollen, sondern nur das für den Anwendungsfall relevante.[222]

Zusammenfassend kann das das Kriterium Service und Support die Akzeptanz auf Seiten der Clients durch folgende Faktoren positive beeinflussen:

- Gewährleistung nachträglicher Verbesserungen und Korrekturen der Lösung.
- Kostenfaktor verringern[223] durch automatische Fehlerbehebung mithilfe von Updates.
- Erfolgswahrscheinlichkeit der Updates durch ausgereiftes Zugriffsmanagement erhöhen.[224]

Letzteres gestaltet sich schwierig, da manche Fenster bei Treiberinstallationen nicht unterbunten werden können. Die Nutzer der Lösung können diese in dem Zeitrahmen der Installation nicht verwenden, da die Installation vordergründig abläuft. Diese Gegebenheit wirkt sich negativ auf die geforderte Benutzerfreundlichkeit aus.[225] Daraufhin lässt sich resistentes Verhalten der Nutzer*innen erkennen, wie auch beispielsweise durch die folgende Aussage von IP7:

> *Denn wir stellen immer mehr und mehr fest, dass viele Anwender, wenn man quasi ein Update anbietet, [. . .] dass viele Anwender sich schwertun, dieses Update zu installieren, weil sie immer die Gefahr sehen, funktioniert mein System danach noch?*[226]

Besonders das Gebiet der Updates muss je nach Einsatz der Client Security Lösung differenziert betrachtet und untersucht werden. Dabei sollte evaluiert werden, inwiefern regelmäßige Updates vonnöten sind und diese den Kunden einen Mehrwert generieren. Außerdem hat sich bei der Untersuchung der Interoperabilität herausgestellt, dass Updates aufgrund des Eingriffs in eine Architektur betriebener Systeme ein äußerst kritischer Faktor in Bezug auf Fehleranfälligkeit und damit auf den anfallenden Mehraufwand (Kosten) darstellen.[227] Andererseits garantieren Updates eine längerfristige Aktualität und Sicherheit der Client Security Lösungen.

4.7 Modell der Auswahlkriterien der Client Security Lösungen

Aus der im vorherigen Abschnitt offengelegten Ergebnisse leiten sich in Kombination mit den vorgestellten Theorien der Akzeptanz[228] und Resistenz[229] verschiedene Hypothesen ab, welche im Folgenden anhand des in Abbildung 3 dargestellten Modells erläutert werden. In das

[222] Vgl. IP8 2021
[223] Vgl. Abschnitt 4.3
[224] Vgl. IP8 2021
[225] Vgl. Abschnitt 4.5
[226] IP7 2021, Z. 478-481
[227] Vgl. Abschnitt 4.1
[228] Vgl. Abschnitt 2.1
[229] Vgl. Abschnitt 2.2

Modell sind alle untersuchten Auswahlkategorien der Client Security Lösung mit eingeflossen, die bereits für die deduktive Auswertung[230] des erhobenen Datenmaterials genutzt wurden. In der Analyse der Zusammenhänge der Auswahlkategorien konnten insgesamt sieben Hypothesen aufgestellt werden, welche in Abbildung 3 und in der folgenden Erläuterung mit *H1* bis *H7* indiziert werden.

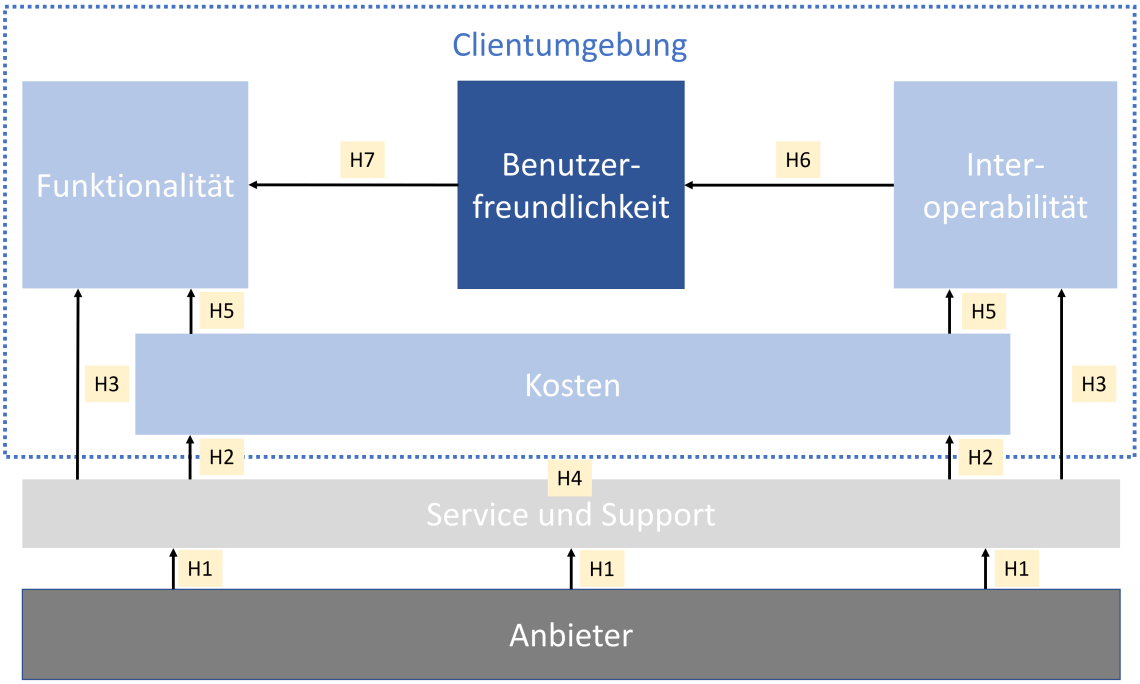

Abb. 3: Modell der Auswahlkategorien von Client Security Lösungen.

H1: Anbieter wird über Service und Support zum strategischen (längerfristigen) Partner.

Die erste Hypothese H1 baut auf den Aussagen der Expert*innen auf, dass sowohl die Aktivität des Anbieters in Form von Innovationen und Updates als auch die beratende Unterstützung bei Fragen und Problemfällen ein Kriterium für die Client Security Lösungen darstellen. Aufgrund der Langfristigkeit, mit der die getroffenen Auswahlentscheidungen von Client Security Lösungen angesetzt werden, können sich auch für den Anbieter Vorteile durch das Angebot von Service und Support etablieren. Für den Anbieter stellt sich die Service und Support als vorteilhaft heraus, wenn Service und Support durch die Wertschätzung des Kundenunternehmens einerseits zu einer längerfristigen Partnerschaft führen und damit garantierte Umsatzerlöse, sofern Lizenzmodelle eingesetzt werden, für den Anbieter darstellen. Anderenfalls kann durch die Wertschätzung des Kundenunternehmens die Möglichkeit gegeben sein, die Service- und Supportleistungen gegen eine monetäre Gegenleistung anzubieten, wodurch die Qualität der Leistungen und Zufriedenheit des Kundenunternehmens steigen können. Die beschriebenen Mechanismen haben somit eine Verwobenheit und intensive Kooperation von Anbieter

[230] Vgl. Abschnitt 3.3 und Abschnitt 3.5

und Kundenunternehmen zur Folge, sodass der Anbieter zum strategischen Partner wird.

H2: Service und Support senken die Kosten.

Dadurch, dass Service und Support die ständige Betriebsfähigkeit einer Lösung unterstützen und Anbieter fachlichen Rat zu bestimmten Problemen geben können, verringern sich die aus Betriebsstillständen, Wartungsarbeiten und Fehlerbehebungen anfallenden Kosten. Außerdem kann eine ausgeprägte Form von Service und Support einzelne Mitarbeiter*innen des Kundenunternehmens in spezialisierte Schlüsselrollen heben und zu Experten für die Client Security Lösung machen. Dadurch werden zwei resistenzverringernde Maßnahmen eingesetzt. Zum einen impliziert das Szenario eine offene Kommunikation zwischen dem Anbieter, der spezialisierten Person und dem Kundenunternehmen. Die spezialisierte Person übernimmt also eine tragende Vermittlungsrolle und kennt sich in der Thematik der Client Security Lösung und der eigenen Unternehmensstruktur sehr gut aus. Zum anderen versetzt das beschriebene Szenario die spezialisierte Person in eine aufgaben- und verantwortungsbezogene Rolle, wodurch eine Integration etabliert wird, die möglichen Resistenzen entgegenwirkt. Generell kann der Abbau von Resistenz zu einer Minderung der Kosten führen, da ausgeprägte aktive und aggressive Resistenzverhalten die Nutzung und Funktionalität der Client Security Lösung schmälern. Im Extremfall kann boykottierendes Verhalten in Form von herbeigeführten Betriebsstörungen und anderen Fehlern zu erhöhten Kosten führen.[231] Im Umkehrschluss senken Service und Support die Kosten, solange die Kosten für die Leistungserbringung nicht die möglichen Aufwände der Fehlerbehebung (etc.) übersteigen.

H3: Service und Support ermöglichen Funktionalität und Interoperabilität.

Service und Support unterstützen das Kundenunternehmen bei Fehlerbehandlungen und anderen Systemausfällen, die auf der eingesetzten Client Security Lösung beruhen. Dadurch können Service und Support die Funktionalität der Lösung im Betrieb des Unternehmens sicherstellen. Aufgrund der Herausforderungen der Interoperabilität, eine Client Security Lösung funktional zu verstehen, zu implementieren und zu betreiben, werden nach Aussagen der Expert*innen Support und Service des Anbieters erfordert. Wenn durch den Support eine Weiterbildung der Mitarbeiter*innen des Kundenunternehmens vollzogen wird, so lassen sich damit möglicherweise bestehende Resistenzen abbauen.[232]

H4: Service und Support mindern das Potential, Resistenzen zu entwickeln.

Generell können Service und Support durch die Etablierung von offener Kommunikation und der Integration und Fortbildung von Mitarbeiter*innen des Kundenunternehmens Resistenzen abbauen.[233] Als Grundlage dafür muss eine Interaktion und Kommunikation auf Augenhöhe zwischen Ansprechpartner*innen des Kundenunternehmens mit der Service und Support

[231] Vgl. Abschnitt 2.2
[232] Vgl. Abschnitt 2.2
[233] Vgl. Abschnitt 2.2

Abteilung gefördert werden. Entsprechend muss auch eine Ausrichtung des Kundenunternehmens an die Interaktions- und Kommunikationsschnittstelle des Service und Support erfolgen.

H5: Kosten wirken als limitierender Faktor auf Funktionalität und Interoperabilität.

Die zweite Hypothese beruht auf der Tatsache, dass die Expert*innen den beschränkenden Mechanismus der Kosten hervorgehoben haben. In Bezug auf die Limitierung der Funktionalitäten wurde geschildert, dass die Unternehmen zwar für die Gewährleistung der Sicherheit einstehen wollen, jedoch die Kosten eine Einschränkung dieser idealisierten Sichtweise herbeiführen. Infolge dessen lässt sich anhand der Aussagen der Expert*innen ableiten, dass sich mit einem gewissen Niveau an Sicherheit zufriedengegeben und nicht die größtmögliche Sicherheit angestrebt wird.
Hinsichtlich der Interoperabilität äußert sich eine Gratwanderung, weil die Unternehmen einerseits gewisse Anforderungen an die Interoperabilität einer Lösung[234] haben, andererseits die Interoperabilität der Client Security Lösung im Vorhinein ressourcenintensiv getestet werden muss, sodass die Menge und Komplexität der Interoperabilität durch die veranschlagten Planungs-, Test-, und Implementierungskosten des Kundenunternehmens limitiert sind.[235]

H6: Interoperabilität erhöht Benutzerfreundlichkeit.

Die Hypothese folgt der Argumentation, dass Kommunikation durch Datenaustausch prinzipiell nur über die Interoperabilität von Systemen möglich ist. Außerdem erhöht die Kommunikationsfähigkeit verschachtelter Systeme und Lösungen zunächst die Möglichkeiten der Nutzung, sodass in einer bestimmten Ausprägung die Benutzerfreundlichkeit erhöht werden kann. Beispielsweise erhöht sich für Administrator*innen die Benutzerfreundlichkeit, wenn verschiedene Client Security Lösungen mithilfe einer zentralisierten Managementlösung kontrolliert werden können und die Administrator*innen nicht verschiedene Lösungen einzeln im Blick behalten muss. Das wohl bekannteste Szenario dieser Hypothese ist die Automation von Maschine-Maschine-Kommunikation, die den Nutzenden einer Lösung verschiedene Arbeitsschritte abnimmt und damit die Benutzerfreundlichkeit erhöht.

H7: Die Benutzerfreundlichkeit erhöht die Funktionalität.

Diese Hypothese wird aus TAM aufgegriffen und anhand der Client Security Lösungen instanziiert.[236] Client Security Lösungen werden in großen Unternehmen meist von Administratoren verwaltet, welche sich folglich in ihrer täglichen Arbeit mit Client Security Lösungen auseinandersetzen und damit die Funktionalität der Lösung für das nutzende Individuum aufgrund der

[234] Beispielweise die Protokollierung von Ereignissen in eine separate Datenbank (Vgl. IP2 2021)
[235] Es wird davon ausgegangen, dass sich die Aufwände für Implementierung und Planung mit steigender Menge und Komplexität der Interoperabilität erhöhen.
[236] Vgl. Abschnitt 2.1

geringeren physischen und mentalen Anstrengungen steigt.[237] Des Weiteren kann die Hypothese als negierte Form des beschriebenen Extremszenarios von IP2 verstanden werden: „Aber wenn man eine Sicherheitslösung nicht bedienen kann, dann nutzt die beste Sicherheitslösung nichts.“[238]

[237] Vgl. Davis 1985, S. 25
[238] Vgl. IP2 2021, Z. 27 f.

5 Evaluation von HP Sure Admin

Zielsetzung: Das folgende Kapitel behandelt die interpretierende Anwendung der in Kapitel 4 erschlossenen Auswahlkriterien von Client Security Lösungen auf die HP-Lösung *Sure Admin*. Wie bereits Kapitel 1 einleitend aufgezeigt, wird das Ziel verfolgt, mithilfe der gewonnen Datenerhebungen in Kombination mit der untersuchten Literatur einen Evaluationsrahmen für Client Security Lösungen zu definieren, der in diesem Kapitel in der Spezifität von HP Sure Admin Verwendung findet. Das Ziel dieses Kapitels ist es, herauszufinden, wie HP Sure Admin aus einer verallgemeinernden Kundensicht zu beurteilen ist und inwiefern die fixierten Auswahlkriterien von Client Security Lösungen erfüllt werden. Abschließend soll mithilfe des Abgleichs der Auswahlkriterien und der tatsächlichen Manifestation von HP Sure Admin festgestellt werden, welche Nutzenpotentiale die Lösung bietet und welche Hemmnisfaktoren diesen gegenüber stehen.

Aufbau: Als erstes wird die Lösung HP Sure Admin anhand von Rahmenbedingungen vorgestellt und der Zweck sowie Einsatzgebiete der Lösung erläutert. Als zweites werden nacheinander die Auswahlkategorien der Client Security Lösungen auf Erfüllung in HP Sure Admin geprüft. Der Abgleich erfolgt erst deskriptiv, indem die betreffenden Aspekte von Sure Admin vorgestellt werden, und wird auf dieser Grundlage anschließend interpretativ je Kategorie beurteilt. Wie aus Abschnitt 4.7 hervorging, stehen die Kategorien dabei in sich wechselseitig beeinflussenden Beziehungen zueinander.

5.1 Zweck und Einsatz von HP Sure Admin

Da Sure Admin im Aufbau recht komplex ist und auf bereits bestehenden HP-Lösungen aufbaut, wird ein grober Überblick über die Architektur des Lösungsansatzes aufgezeigt.

HP bietet mit Sure Admin eine neuartige Zweckermöglichung des BIOS-Schutzes an. Grundlegender Aspekt der Lösung ist die zertifikationsbasierte Verschlüsselung des BIOS, welche die Sicherheit und das Management des BIOS-Zugriffs verbessern soll. Die Lösung beinhaltet ein Framework, welches Ansätze der Zertifikatserstellung und -speicherung bis hin zum Management der Zertifikate und des Zugangs enthalten.[239]

Das Management und die Kontrolle der Implementierung und des Betriebs von Sure Admin werden durch zwei verschiedene Komponenten sichergestellt. Zum einen existiert die HP-Lösung Manageability Integration Kit (MIK), welche als ein Plug-In für das Verwaltungswerkzeug System Center Configuration Manager (SCCM) vertrieben wird. Zum anderen kann das von HP entwickelte und vertriebene PowerShell-Modul Client Management Script Library (CMSL) genutzt werden. Beide Verfahren setzen einen Download mit anschließender Installation der Komponente voraus.

[239] HP Inc. 2021b

Zum Erstellen und Speichern der Zertifikate verwenden beide genannten Verfahren die HP-eigene Lösung Secure Platform Management (SPM), welche vor der Nutzung von Sure Admin im BIOS freigeschaltet werden muss. SPM ist eine kryptografisch sichere Infrastruktur, in welcher die Public-Key-Kryptografie[240] zur Ver- und Entschlüsselung verwendet wird.[241]

Sure Admin etabliert zwei Verfahren zur Entschlüsselung des BIOS. Einerseits ermöglicht die Lösung den Remote-Zugriff auf das BIOS, durch welchen Einstellungen am BIOS und die Installation von Updates aus zentraler Hand vorgenommen werden können.
Andererseits kann das Remote-Management durch eine lokale Zugangsmöglichkeit (Local-Access) erweitert werden, sodass der Zugriff auf das BIOS entweder direkt am Client oder über Remote-Management erfolgen kann.[242] Der lokale Zugang erfolgt in der kombinierten Nutzung von zu entsperrendem Client und einem Smartphone. Wird beim Boot-Vorgang des Clients das BIOS aufgerufen, erscheint ein QR-Code, den es mit der Smartphone-App „Sure Admin“ zu scannen gilt. Nachdem der Code erfolgreich gescannt wurde, wird ein Einmalpasswort für den Client generiert.[243]

Für die Erstellung des Einmalpassworts wird ein so genannter Local Access Key (LAK) verwendet, der auf zwei verschiedenen Wegen integriert werden kann. Zum einen kann der LAK auf die entsprechenden Smartphones via Email oder Ähnlichem verteilt werden. Bei diesem Ansatz ist keine Internetverbindung des Smartphones notwendig, um das Einmalpasswort erstellen zu können.
Zum anderen kann die Generierung in Verbindung mit einer Cloudlösung implementiert werden, sodass auf den Smartphones keine Zertifikate oder anderen sensiblen Daten gespeichert werden müssen. Beim Cloudansatz werden die Private-Keys (LAKs) in einer speziellen für das Schlüsselmanagement ausgelegten Umgebung gespeichert.[244] Anwender*innen, welche das BIOS in diesem Szenario entschlüsseln wollen, scannen erst den QR-Code auf dem Client ab und werden dann zu einer Anmeldeseite der Cloud weitergeleitet. Sobald die Nutzer*innen die Autorisierung durch die Eingabe der Zugangsdaten bestätigt haben, wird ein Einmalpasswort generiert und auf dem Smartphone ausgegeben. Dieses Einmalpasswort kann nun auf dem Client eingegeben werden, sodass anschließend das BIOS entsperrt wird.

[240] Dazu wird eine bereitgestellte Nutzlast durch einen Private-Key signiert, wobei das Zielsystem (Client) den dazugehörigen Public-Key verwendet, um die Legitimität der Signierung zu überprüfen.
[241] Vgl. HP Inc. 2021c, S. 3
[242] Wird Local-Access nicht implementiert, so ist der Zugang Vorort am Client unter keinen Umständen, sondern nur über die Nutzung des Remote-Managements möglich.
[243] Vgl. HP Inc. 2021c, S. 7
[244] HP Inc. 2021a

5.2 Anwendung des Bewertungsmodells auf HP Sure Admin

Anbieter

Die befragten Expert*innen nannten als ein entscheidendes Kriterium für die Wahl einer Client Security Lösung die Referenzen des Anbieters für erfolgreiche Einsätze der Lösung. Für Sure Admin gibt es bisher keine solcher Referenzen, welche die Qualität der Lösung belastbar bestätigen würden. Damit sich das Fehlen solcher Referenzen nicht negativ auf die Bewertung potenzieller Kunden auswirkt, müssen andere Vertrauen schaffende Faktoren bereitgestellt werden.

Die fehlenden Erfolgsbeispiele der Lösung können durch unmittelbare Erfahrungen mit Sure Admin kompensiert werden, welche den Kund*innen den Nutzen greifbar aufzeigen. Diese Nutzenerfahrungen ersetzt dann in Teilen das Vertrauen, welches nicht durch Referenzen gewonnen werden konnte. Solche Erfolgsbeispiele können durch Proof of Concept (POC)s verwirklicht werden. In einem POC werden neue, unerprobte Lösungsansätze prototypisch umgesetzt und anschließend der funktionale Erfolg der Lösung und deren Eignung bewertet. Somit wäre es möglich, den Kund*innen ohne großes finanzielles und funktionales Risiko in einer Testumgebung darzulegen, wo die Vorteile und wo die Herausforderungen liegen, damit sie sich selbst von der Lösung überzeugen können. Ein solcher POC ist jedoch nur bei ausreichend großen Kunden möglich, da ansonsten der Kostenfaktor für den POC die Rentabilität des gesamten Geschäfts stark negativ beeinflusst.

HP genießt durch die Reputation und die langjährige Erfahrung in der Branche grundsätzlich ein gewisses Vertrauen, welches jedoch bei solch tiefgreifenden Eingriffen in Kernprozesse nicht vollkommen ausreichend ist. Trivial lässt sich das generelle Vertrauen in die Kompetenz von HP als Anbieter damit belegen, dass die befragten Kundenunternehmen augenscheinlich Produkte von HP einsetzen. Die notwendige Überzeugung für die Lösung variiert in Abhängigkeit davon, wie die Unternehmen generell Innovationen gegenüber eingestellt sind. Dieser Argumentation folgend werden Innovationen erst sehr spät in den jeweiligen Unternehmen adaptiert, sobald viele andere Unternehmen die Innovation getestet und für gut befunden haben. Dies steht jedoch im Widerspruch zu dem Anspruch aus den Aussagen der Befragten, aktuelle Sicherheitslösungen einsetzen zu wollen. Diese aktuellen Lösungen sollen die Umsetzung bestimmter Normen, die beispielsweise von der BSI vorgegeben werden, beinhalten und müssen damit einhergehend eine gewisse Neuheit besitzen. Genau diese Neuheit stellt wiederum für die Kund*innen ein Problem dar. In Bezug auf HP selbst sind einige Aussagen der Expert*innen auffällig, die auf eine Unzufriedenheit mit HP hinweisen. Diesbezüglich wurde angeführt, dass HP an seiner Transparenz zu den Kund*innen arbeiten soll und insbesondere die Dokumentation von Lösungen übersichtlicher und ausführlicher gestaltet werden soll. Das Argument der Offenheit sollte von HP berücksichtigt werden, da eine offene Kommunikation mit den Anwender*innen einer Lösung zur Reduktion von existierenden Resistenzen

beiträgt.[245]

Der Forderung, eine Client Security Lösung muss mindestens für die Dauer eines Lebenszyklus eines Clients eingesetzt werden können, kommt der Mechanismus entgegen, dass HP einen Teil der Implementierung von Sure Admin ab Werk anbietet.

Kosten

Sure Admin wird von HP kostenlos zur Verfügung gestellt, sodass für Kunden weder einmalige Anschaffungskosten noch Lizenzkosten für die Nutzungsrechte anfallen. Sure Admin bringt jedoch durch den neuartigen Ansatz der Zertifikatsauthentifizierung im BIOS einige Änderungen in tiefgreifenden Prozessen der Kundensysteme mit sich. So ändert sich durch Sure Admin nicht nur die Zugangsart von einem Passwortansatz zu einem Zertifikatsansatz. Die Speicherung und Verwaltung der Zertifikate in der SPM des Nutzer-Geräts bedeuten einen Mehraufwand und die Integration des Authentifizierungsprozesses von Sure Admin Veränderungen in den alltäglichen Arbeitsschritten der Administrator*innen.

Solche systemischen Veränderungen stellen Gründe für Resistenzen aufgrund der Verschlechterung der Benutzerfreundlichkeit durch eine höhere Komplexität im Authentifizierungsprozess dar, die es als Anbieter zu vermeiden gilt.[246] Eine solche Verschlechterung der direkt wahrgenommenen Benutzerfreundlichkeit für Administrator*innen bei systemischen Umstrukturierungen können durch HP in Form von standardisierten Integrationsansätzen und Schritt-für-Schritt-Anleitungen unterstützt werden, damit die Mitarbeiter*innen des Kundenunternehmens weniger Aufwand mit dem Integrieren und Erlernen haben. Wie hoch die tatsächlichen Kosten während des Betriebs infolge von eventuellen Fehlerbehandlungen, Anpassungen und Ausfällen sind, kann aufgrund der fehlenden Referenzen und der Neuartigkeit der Lösung schwer abgeschätzt werden. In den Aussagen der Befragten waren die Anschaffungs- und Lizenzkosten zusammen mit den Kosten für manuelle Nacharbeiten in Bezug auf alle Client Security Lösungen die gewichtigsten Kostenfaktoren. Daraus folgt für die untersuchte Lösung dieser Arbeit, dass für eine sinnhafte und belastbare Kostenabschätzung von Sure Admin nicht nur die direkten finanziellen Kosten einer Integration einkalkuliert werden müssen, sondern verstärkt auch der Aufwand für jeden einzelnen in dem Umgang mit dem System. Sobald sichergestellt ist, dass der Prozess der Authentifizierung eine ausreichende „Perceived Usefulness“ erzielt, kann die Kostenabschätzung durch nicht vorhandenen Lizenzkosten und abschätzbaren Deployment Kosten klar kommuniziert werden.

Funktionalität

Die Funktionalität von Sure Admin lässt sich auf einen Kernbereich konzentrieren. Es bildet eine Sicherheitsebene um das BIOS, die eine kontrollierte Zugriffsregulation beinhaltet.

[245] Vgl. Abschnitt 2.2
[246] Vgl. Abschnitt 2.2

Der Hauptanwendungsfall liegt in dem Updateprozess des BIOS, über welchen neben den standardmäßigen Konfigurationen des BIOS auch der autorisierte Zugang festgelegt wird. Bezüglich der Zugangskontrolle ermöglicht Sure Admin gänzlich neue Ansätze zu herkömmlichen Passwort-Lösungen. Die Verwendung von Zertifikaten bedeuten eine deutlich erhöhte Sicherheit durch die Abschaffung von testbaren Passwörtern und anderen Authentifizierungs-Missbräuchen (social Engineering). Durch die Nutzung von MIK und CMSL wird die automatische Verwaltung von Sure Admin ermöglicht, was eine der Auswahlkriterien der Kunden für oder gegen eine spezielle Client Security Lösung abbildet. Neben der Automation ist ein entscheidender funktionaler Vorteil von Sure Admin die Nutzung von zeit- und gerätelimitierten Einmalpasswörtern. Diese Einmalpasswörter stellen aufgrund ihrer Charakteristika einen entscheidenden Vorteil gegenüber Standardpasswörtern dar, da solche Passwörter häufig auf allen Geräten identisch sind und selten ausgetauscht werden. Die standardmäßig eingesetzte Implementierungsform stellt die Local-Access-Lösung unter Verwendung der Cloud dar. Einige Expert*innen bemängelten jedoch, dass aufgrund der ständigen lokalen Verfügbarkeit und der Sicherheitsproblematik bei ausgelagerten Daten in der Public Cloud[247] der Bedarf für einen lokalen, unabhängigen Ansatz besteht.[248] Als eine passende Lösung dieser Problematik kann die Local-Access Lösung ohne Cloudintegration eingesetzt werden. Allerdings entsteht durch die Verteilung der LAKs auf die einzelnen Smartphones ein erhöhter Aufwand im Bereich des Key-Management und ein Kontrollverlust über die zentrale Verteilung der Schlüssel. Die grundlegende kryptografische Sicherheit der erstellten Schlüssel ist durch das anerkannte und zertifizierte Verfahren des SPM gesichert.

Interoperabilität

In der Untersuchung der Interoperabilität stellt sich die grundlegende Frage, ob sich die Verknüpfung vieler Lösungen und Werkzeuge als nützlich für Benutzer*innen herausstellt. Je mehr Schnittstellen vorhanden sind, desto mehr Möglichkeiten des Datenaustauschs bestehen und desto besser kann die eigene Lösung in weitere Werkzeuge integriert werden und beispielsweise in einem zentralen Aktions-Logging Informationen beitragen. Dieser Vorteil wird jedoch dadurch gedämpft, dass die Komplexität der möglichen Datenströme die Schwierigkeit der Implementierung erhöht und die Ausfallsicherheit aufgrund der steigenden Anzahl an Fehlerquellen verschlechtert.

Auf den Einsatz von MIK und CMSL bezogen, bedeutet der Kontext der Interoperabilität zunächst mehr Integrationsfreiheiten für die Nutzenden. Für HP als Anbieter dieser Schnittstellen ergibt sich jedoch eine Doppelbelastung durch höhere Entwicklungskomplexität und größeren Wartungsaufwand. Dieser Aufwand stellt jedoch nur indirekt durch eventuell erhöhte Kosten eine Hinderung für die Kund*innen dar.

[247] Bei Sure Admin wird die Verwendung von Microsoft Azure aufgrund der Implementierung der Schlüsselmanagementumgebung vorausgesetzt.
[248] Vgl. IP3 2021, Vgl. IP4 2021, Vgl. IP6 2021

Benutzerfreundlichkeit

Die Expert*innen führen an, dass zumeist Remote-Lösungen in den Unternehmen eingesetzt werden. Diese Remote-Lösung bietet durch einheitliche Anbindung an die Clients und zentrales Management der Zugriffe eine erhöhte Benutzerfreundlichkeit. Zusätzlich lässt sich festhalten, dass den Kund*innen, aufgrund der unterschiedlichen Integrationsarten von Sure Admin, Freiheiten eingeräumt und subjektive Präferenzen in Bezug zur Benutzerfreundlichkeit berücksichtigt werden können. Beispielsweise kann für die eine Person ein Konsolenansatz des Remote-Managements benutzerfreundlicher wirken als der Local-Access-Ansatz. Unabhängig davon würde den Angaben der Expert*innen zufolge der Einsatz der Local-Access-Lösung den Arbeitsalltag der Anwender*innen beeinträchtigen, da diese während der Änderungen den Client nicht auf andere Weise nutzen können. Der Ausfall an Arbeitszeit wird als ein Mangel an Benutzerfreundlichkeit angesehen.[249]

Außerdem gaben Unternehmen mit einer hohen Anforderung an Sicherheit an, dass der Einsatz von Cloud-Lösungen den Anspruch der vertraulichen Handhabung der Daten durch den Cloudbetreiber nicht immer und zuverlässig erfüllen kann.[250] Daraus folgt die Nachfrage nach einer lokalen, cloud-unabhängigen Lösung. Diese Lösung bringt einige Unannehmlichkeiten, wie zum Beispiel kein zentrales Management mit sich, die gewissermaßen im Austausch für erhöhte Sicherheit auftreten.

Service und Support

Alle befragten Expert*innen haben dem Service und Support einen hohen Stellenwert eingeräumt. Der Service zeichnet sich durch die Erreichbarkeit und Unterstützung des Anbieters zu Fehlerbehebungen in Integration und Betrieb aus. Hinsichtlich Sure Admin und dem angebotenen Support seitens HP lässt sich festhalten, dass bisher kein dedizierter Support für Sure Admin angeboten wird und Fragen der Kund*innen individuell durch die HP-Expert*innen beantwortet und gelöst werden. Aufgrund des kostenfreien Angebots scheinen der mangelnde Service und Support einleuchtend zu sein. Es stellt sich jedoch die Frage, ob nicht die Bepreisung und die Einführung von Service und Support den Mehrwert der Lösung steigern würden. Es lässt sich festhalten, dass es insbesondere bei dieser Kategorie schwer ersichtlich ist, wie viel Support tatsächlich von den Kundenunternehmen eingefordert werden würde und wie fehleranfällig die Lösung im tatsächlichen Betrieb ist.

[249] Vgl. IP2 2021
[250] Vgl. IP4 2021

6 Resümee und kritische Betrachtung

In diesem Kapitel soll die Vorgehensweise zur Erfüllung der gesetzten Ziele und der Beantwortung der Forschungsfrage kritisch reflektiert und in den Kontext der wissenschaftlichen Forschung eingeordnet werden.

Die in Kapitel 1 erläuterten Zielsetzungen der Arbeit sollten der Lösungsfindung zur Problemstellung, auf Grundlage welcher Auswahlkriterien eine Kaufentscheidung von Client Security Lösungen getroffen wird, dienen. Dazu wurde die Struktur und der Inhalt dieser Arbeit anhand der gesetzten Forschungsfrage reflektiert:

> ***Welche Nutzenpotenziale und Resistenzfaktoren stehen sich bei der Entscheidungsfindung von Kund*innen zum Einsatz einer Client Security Lösung gegenüber?***

Das Forschungsdesign dieser Arbeit baute auf einer Untersuchung der wissenschaftlichen Literatur auf, die das Berücksichtigen von bestehenden und erforschten Lösungsansätzen gewährleisten sollte. Darauf aufbauend wurde eine qualitative Erhebung zur Analyse von Kriterien der Client Security Auswahl durchgeführt. Mithilfe der Methodik der deduktiven Auswertung wurden anschließend Erkenntnisse aus dem Datenmaterial generiert. Konkret wurde in Kapitel 2 zunächst die wissenschaftliche Literatur zu Theorien der Akzeptanz und Resistenz untersucht, um damit Hinweise auf das Verhalten und die zugrundeliegenden Ursachen von Individuen zu erhalten. Mithilfe der Theorien zu Akzeptanz und Resistenz wurde eine Argumentationsbasis für die Bewertung einzelner Auswahlkriterien in den folgenden Untersuchungen dieser Arbeit geschaffen.

Kritisch muss dabei betrachtet werden, inwiefern die empirisch erschlossenen Ursachen von Akzeptanz und Resistenz das tatsächliche Verhalten von Kund*innen beeinflussen. Insbesondere in der Auswertung der Interviewdaten konnte festgestellt werden, dass die Sicherheitsanforderungen und im Besonderen das Erfüllen von Normen teils auf rechtlichen Grundlagen beruhen und nicht aus subjektiven Verhaltensweisen hervorgehen.

Hinsichtlich der herangezogenen Auswahldimensionen der ERP-Auswahl muss prinzipiell davon ausgegangen werden, dass die definierten Dimensionen nicht die Gesamtheit aller von den Kund*innen berücksichtigter Kriterien abbilden. Um dieser Möglichkeit der unvollständigen Betrachtungsperspektiven gerecht zu werden, wurde in der Auswertung der Interviewdaten bewusst die Möglichkeit offengehalten, weitere Perspektiven in Form von Auswertungskategorien zu berücksichtigen. Die Auswertung der erhobenen Daten hat so zu der Bildung einer weiteren Kriterienkategorie geführt. Die Analyse der Interviewdaten hat ergeben, dass Service und Support als Bindeglied zwischen Kundenunternehmen und dem Anbieter der Client Security Lösung eine leittragende Rolle für die Akzeptanz und Resistenz der Lösung zukommt.
Es müssen zudem die Ergebnisse der Interviewauswertung kritisch betrachtet werden, um deren Aussagequalität beurteilen zu können. Im Rahmen der Interviews wurden ausschließlich

bestehende Kunden von HP befragt, sodass die Ergebnisse auf einer sehr spezifischen Zielgruppe beruhen. Insbesondere die Wichtigkeit des Anbieters und die Rolle von Service und Support verdeutlichen die zentrale Rolle des Anbieters in den vorgestellten Ergebnissen und legen eine kontextbedingte Beeinflussung der Expert*innenaussagen nahe. In Bezug auf die Auswahl der Expert*innen muss festgehalten werden, dass vor allen Dingen Personen aus den Bereichen der Client-Architektur befragt wurden. Eine breitere Berücksichtigung verschiedener Rollen hätten so womöglich andere Ergebnisse ergeben. In diesem Maße sind die festgestellten Auswahlkriterien auf die Sichtweise der Expert*innen limitiert. Um in weitergehenden Untersuchungen diesen Kritikpunkten, welche die Qualität der Ergebnisse betreffen, entgegen zu wirken böten sich Mixed-Method-Ansätze an, welche die hervorgebrachten Ergebnisse durch eine weiterführende quantitative Erforschung beurteilen können. Auf diese Weise sollte insbesondere die Überprüfung der in Abschnitt 4.7 erläuterten Hypothesen in Betracht gezogen werden.
Mit einer quantitativen Untersuchung kann so die Gültigkeit der aufgestellten Hypothesen in einem breiteren Untersuchungskontext, unabhängig von den genannten Einschränkungen der hier beschriebenen Forschung, analysiert werden. Aus dieser quantitativen Untersuchung kann eine Falsifikation der vorgestellten Ergebnisse durchgeführt werden, die aufgrund des zweistufigen Erhebungsverfahrens belastbarere Aussagen treffen kann.

Die Evaluierung der Ergebnisse hat einige Erkenntnisse hervorgebracht, an denen sich für eine erfolgreichere Einführung der untersuchten Plattform in neuen und bestehenden Kundenumgebungen orientiert werden kann. Nicht nur wurden greifbare Aspekte, wie die Relevanz einer erreichbaren oder grundsätzlich vorhandenen Unterstützung durch den Support identifiziert, sondern auch Aspekte, die in der Sache selbst verankert sind und gleichzeitig hinderlich für eine Einführung sind. Hierbei ist der Aspekt der Sicherheit zu Lasten der Benutzerfreundlichkeit zu nennen.
Da die Steigerung der Sicherheit Hauptziel von Sure Admin ist kann diese Funktionalität nicht angepasst werden, sondern es muss durch andere Aspekte der Verlust an Vertriebsaspekten aufgewogen werden. Alle Faktoren, die in der Evaluation gefunden wurden, sind spezifisch für den Fokus der Untersuchung und können auch nur belastbar in diesem angewendet werden. Um in anderen Gebieten eine ähnliche Aussage treffen zu können, muss die Methodik entsprechend neu evaluiert werden und die Vorgehensweise mit dem Ergebnis angepasst werden. Die Faktoren beantworten den Schritt, der auf die Forschungsfrage folgt, nämlich womit und wie gefundene Ursachen der Akzeptanz und Resistenz auf die Nutzung einer Client Security Lösung förderlich oder hemmend wirken.

Anhang

Anhangverzeichnis

Anhang 1 Leitfaden 58
Anhang 2 Muster Interview-Einwilligungserklärung 61
Anhang 3 Gesprächsverzeichnis 62
Anhang 4 Kodierleitfaden 63
Anhang 5 Interview-Transkripte 65
- Anhang 5/1 Interview mit Interviewpartner 1 (IP1) 65
- Anhang 5/2 Interview mit Interviewpartner 2 (IP2) 75
- Anhang 5/3 Interview mit Interviewpartner 3 (IP3) 84
- Anhang 5/4 Interview mit Interviewpartner 4 (IP4) 91
- Anhang 5/5 Interview mit Interviewpartner 5 (IP5) 98
- Anhang 5/6 Interview mit Interviewpartner 6 (IP6) 101
- Anhang 5/7 Interview mit Interviewpartner 7 (IP7) 108
- Anhang 5/8 Interview mit Interviewpartner 8 (IP8) 122
- Anhang 5/9 Interview mit Interviewpartner 9 (IP9) 132

Anhang 6 Induktive Kategorienbildung von Service und Support 137
Anhang 7 Deduktive Kategorienanwendung 140

Anhang 1: Leitfaden

Vorwort und Einstieg

- Themenvorstellung.
- Es werden meist offene Fragen gestellt, um möglichst reichhaltige und unbeeinflusste Antworten zu erhalten.
- Fühlen Sie sich frei, über das zu sprechen, was Ihnen am wichtigsten ist.
- Definitionen für gemeinsames Verständnis werden erläutert.
- Hinweis zur Einwilligungserklärung (insb. Datenschutzhinweise, Aufnahme).
- Gibt es offene Fragen?

Vorstellung von Rolle und Unternehmen

1. Können Sie bitte Ihre konkrete Position beziehungsweise Ihre Rolle erklären?
    a) Sind Sie verantwortlich dafür, ob und mit welchen Client Security Lösungen das Unternehmen arbeitet?
2. Wie beschreiben Sie die Rahmeneigenschaften Ihres Unternehmens?
    a) Wie beschreiben Sie Ihre Branche?
    b) Welche Anzahl an Clients betreut Ihr Unternehmen?
    c) Wie ist das Client Management organisiert (grob)?
    d) Welche Sicherheitsanforderungen prägen Ihre Entscheidungen bezüglich Client Security Lösungen?
        i. Gibt es branchenspezifische Sicherheitsanforderungen? Wenn ja, welche?
        ii. Gibt es gesetzliche Sicherheitsanforderungen? Wenn ja, welche?
        iii. Gibt es kundenspezifische Sicherheitsanforderungen? Wenn ja, welche?

Erfahrungen mit Client Security Lösungen

3. Welche Client Security Lösungen setzen Sie in Ihrem Unternehmen ein?
4. Welche Lösung haben Sie als letztes eingeführt?
   a) Wie kam es dazu, dass eine neue Lösung eingeführt wurde?
   b) Welche Funktionen hatte die Lösung?
   c) Was war der ausschlaggebende Faktor, der dazu geführt hat, diese Lösung auszuwählen?
   d) Gab es eine Vorgängerlösung? Wenn ja, was waren die Vorteile der neuen Lösung?
   e) Wurden aufgrund der Implementierung der Lösung technischen Prozesse verändert?

Entscheidungsprozess für Client Security Lösungen

5. Gibt es einen Beschaffungsprozess für Client Security Lösungen? Wenn ja:
   a) Wer ist im Entscheidungsprozess involviert? Wie interagieren diese Personen?
   b) Wie langfristig wurden derartige Entscheidungen getroffen?
   c) Gibt es (regelmäßige) Ausschreibungen?

Kriterien und Anforderungen an Client Security Lösungen

6. Welche Rolle spielte der Anbieter für die Auswahl einer Client Security Lösung?
   a) Welche Kriterien muss ein Anbieter erfüllen, damit er in Betracht gezogen wird?
7. Welchen Einfluss haben die Kosten für die Auswahl einer Client Security Lösung?
8. Welche Eigenschaften Ihrer Client Security Lösungen haben dazu geführt, dass die Lösungen ...
   a) für den Benutzer des Clients benutzerfreundlich waren?
   b) für den Administrator der Clients benutzerfreundlich waren?
9. Was bezweckt Ihrer Meinung nach der Einsatz einer Client Security Lösung?

BIOS-Schutz der Clients

10. Schützen Sie das BIOS Ihrer Clients? Wenn ja, wie?
    a) Benutzen Sie ein BIOS-Passwort?
    b) Wie gestaltet sich die Organisation und das Management?
11. Wie sieht Ihrer Meinung nach der ideale Schutz des BIOS aus?

Ergänzungen

12. Gibt es weitere Aspekte, die ihrer Meinung nach wichtig sind und noch nicht erwähnt wurden?

Anhang 2: Muster Interview-Einwilligungserklärung

Ich erkläre hiermit mein Einverständnis zur Nutzung der personenbezogenen Daten, die im Rahmen des folgenden Gesprächs erhoben wurden:

- Forschungsprojekt: Bachelorarbeit zum Thema „Nutzen- und hemmnisorientierte Evaluation einer Client Security Lösung am Beispiel von HP Sure Admin“ im Studiengang Wirtschaftsinformatik – Application Management
- Durchführende Hochschule: DHBW Stuttgart
- Interviewer: Peter Falterbaum
- Datum des Interviews: *dd.mm.yyyy*

Die Daten werden im Rahmen eines digitalen Gesprächs erhoben, welches aufgezeichnet wird. Zum Zwecke der Datenanalyse werden die mündlich erhobenen Daten verschriftlicht (Transkription), wobei die Daten anonymisiert werden. Eine Identifizierung der interviewten Person ist somit ausgeschlossen. Nach dem Abschluss des Projekts werden diese Daten gelöscht. Der Speicherung der personenbezogenen Daten zu Dokumentationszwecken kann durch die interviewte Person jederzeit widersprochen werden. Die Teilnahme an dem Gespräch erfolgt freiwillig. Das Gespräch kann zu jedem Zeitpunkt abgebrochen werden. Das Einverständnis zur Aufzeichnung und Weiterverwendung der Daten kann jederzeit widerrufen werden.

Im Einzelnen bin ich damit einverstanden,

- dass das Interview digital aufgezeichnet wird.
- dass das Interview transkribiert und anonymisiert wird.
- dass alle Angaben, die zu einer Identifizierung der Person führen könnten, verändert oder aus dem Transkript entfernt werden.
- dass Sequenzen des Interviews in transkribierter und anonymisierter Form im Rahmen des oben angegebenen Forschungsprojektes interpretiert werden.
- dass die Transkription in verschrifteter Form für Publikationszwecke der oben genannten wissenschaftlichen Arbeit (Bachelorarbeit) verwendet werden darf.
- dass die zur Verfügung gestellten Daten, die Aufzeichnung und die Transkription bis zum Abschluss des Projekts gespeichert und anschließend gelöscht werden.

Unter diesen Bedingungen erkläre ich mich bereit, das Interview zu geben, und bin damit einverstanden, dass es aufgezeichnet, verschriftlicht, anonymisiert und ausgewertet wird.

_____

Unterschrift: *Name Interviewpartner*

Anhang 3: Gesprächsverzeichnis

IP1 (2021) Senior Workplace Architekt, IT-Dienstleistung für Lebensmitteleinzelhandel, 38 Minuten, Videoanruf via Microsoft Teams, 31.03.2021.

IP2 (2021) System Spezialist Windows, Banken und Finanzdienstleistungen, 30 Minuten, Videoanruf via Microsoft Teams, 06.04.2021.

IP3 (2021) Service Development BIOS und Treiber Management, IT-Dienstleistung für Bundeswehr und Bund, 25 Minuten, Videoanruf via Microsoft Teams, 07.04.2021.

IP4 (2021) Senior IT-Architect, IT-Dienstleistung für Bundeswehr und Bund, 34 Minuten, Videoanruf via Microsoft Teams, 09.04.2021.

IP5 (2021) Systemadministrator, IT-Dienstleistung für Banken, 26 Minuten, Videoanruf via GoToMeeting, 09.04.2021.

IP6 (2021) Product Owner Basic Workplace Windows, IT-Dienstleistung für Verkehr und Logistik, 24 Minuten, Videoanruf via Microsoft Teams, 13.04.2021.

IP7 (2021) Client Installation & HW Validation, IT-Dienstleistung, 54 Minuten, Videoanruf via Microsoft Teams, 14.04.2021.

IP8 (2021) Client Engineering Hardware Zertifizierung, Telekommunikation, 40 Minuten, Videoanruf via Microsoft Teams, 16.04.2021.

IP9 (2021) WS Deployment Client Engineering, Telekommunikation, 18 Minuten, Videoanruf via Microsoft Teams, 16.04.2021.

Anhang 4: Kodierleitfaden

Kategorie	Definition (Literatur)	Ankerbeispiele	Kodierregeln
Kosten	Kosten umfassen in diesem Kontext alle monetären Aufwendungen, welche sich mittelbar oder unmittelbar aus der Anschaffung oder dem Betrieb einer Client Security Lösung ergeben. Die Definition beinhaltet sowohl Aufwendungen an Dritte, die beispielweise durch den Kauf von Leistungen wie Produkten, Lizenzleistungen und Dienstleistungen entstehen können, als auch Aufwendungen, welche innerhalb eines Unternehmens für Implementierungen, Wartungen, Mitarbeiter, Umstellungen oder ähnliches anfallen. Dieser Eingrenzung werden auch kalkulierte, veranschlagte und geplante Aufwendungen (s.g. Budget) zugeordnet.	[...] zum einem natürlich die Kosten, weil wir das dann halt in der International-Cloud kostenlos bekommen. IP8 Wichtig ist es, den Client so sicher wie möglich zu halten, mit so wenig wie möglich Aufwand. IP9 Wenn [mehrere Produkte] alle Anforderungen erfüllen, dann bekommt die kostengünstigste Lösung den Zuschlag. IP6	Die Kategorie enthält alle Aussagen über Budgetvorgaben; Faktoren, welche die Kosten direkt beeinflussen; subjektive Einstellungen zu Kosten und Beschreibungen zu Kostenaufstellungen.
Funktionalität	Funktionalität inkludiert all diejenigen Aussagen, welche den Zweck und die Nutzenstiftung einer Client Security Lösung umschreiben. Darunter fallen Prozesse und Aktionen einer Lösung, die für Nutzenden durch den Einsatz der Lösung einen Mehrwert generieren. Im Kontext der Client Security stellen dies vor allen Dingen Eigenschaften dar, welche die Fähigkeit der Lösung, Informationen und Daten vor unautorisierten Zugriffen und Veränderungen zu schützen. (Vgl. \cite{ISO.2017})	Das ist allein schon die größte Security, weil der User halt einige Sachen einfach nicht darf und machen kann. IP2 Eine Client Security Lösung sollte auf jeden Fall teil-automatisiert und standardisiert sein. IP3 Wir wollen eigentlich komplett passwort-less werden. IP6	Die Kategorie enthält alle Aussagen darüber, welche Mehrwerte aus der Nutzung der Lösung gezogen werden können und die auf mögliche Einsatzgebiete der Lösung hinweisen.
Interoperabilität	Interoperabilität beinhaltet alle Aspekte der Lösung, welche eine Integration in vorhandene System- und Architekturumgebungen bezüglich des Datenaustauschs proaktiv unterstützt. Darunter fallen definierte Schnittstellen und die Umsetzung verbreiteter Standards, welche den Datenaustausch und die Verarbeitung der Daten zu Erfüllung einer bestimmten Gesamtfunktionalität erleichtern. Im Kontext der Client Security umfasst die Definition insbesondere den Schutz der Schnittstellen.	Wir wollen Standardlösungen von renommierten Herstellern, also von den Top-Anbietern, die dann entsprechende Konfigurationsmöglichkeiten bereits mitbringen. IP6 Wenn so eine Sicherheitslösung bei uns einen Benefit bringt, dann sind wir definitiv bereit, unsere Prozesse auch anzupassen, damit diese Lösungen implementiert werden kann. IP4 Das heißt, es müssen nicht nur die User durchgereicht werden, sondern es müssen auch Berechtigungsgruppen durchgereicht werden. IP2	Die Kategorie beinhaltet alle Aussagen zu Client Security Lösungen, welche Schnittstellen, den Datenaustasuch, das Zusammenarbeiten verschiedener Systeme und Produkte oder anbieter- und systemübergreifende Aspekte thematisieren.

Kategorie	Definition (Literatur)	Ankerbeispiele	Kodierregeln
Anbieter	Den Anbieter umschreiben alle Aussagen, welche charakterisitische Eigenschaften eines Anbieters enthalten. Außerdem werden derlei Aspekte dem Anbieter zugeordnet, welche Referenzen, Zertifizierungen und andere Qualitätsmerkmale eines Anbieters thematisieren.	Und natürlich muss der Anbieter nachweisen, dass er auch in der Größe entsprechende Referenzen hat. IP6 Ich bin sogar eher ein Freund, wenn es um Security geht, verschiedene Anbieter zu haben. IP2 Es muss natürlich sichergestellt sein, dass der Anbieter vertrauenswürdig ist. IP4	Die Kategorie umfasst alle Aussagen zu Größe, Referenzen, Expertise, Vertrauenswürdigkeit und Zuverläsigkeit des Client Security Anbieters.
Ease of Use	Die Benutzerfreundlichkeit umfasst eher nicht-funktionale Eigenschaften einer Lösung, welche den Betrieb durch einen Menschen möglichst konstruktiv unterstützt. Es umfasst die Art der Ausgestaltung der Funktionalität und inwiefern diese dem subjektiven Empfinden eines Individuums entgegen kommt.	Mehr Dokumentation wünschen wir uns von einem Hersteller. IP4 [Wir bewerten] Tools [gut], die man mal schnell testen kann, die auch schnell funktionieren. IP8 [Im Optimalfall schaut] der Administrator nur irgendwie auf eine Konsole, schaut, dass alle meine Clients auf dem aktuellen Stand [sind] und vielleicht noch sieht, okay, da war jetzt ein Virus. IP9	Die Kategorie umfasst alle Aussagen zu den Eigenschaften der Benutzerfreundlichkeit, welche die Nutzung einer Lösung mit Adjektiven wie intuitiv, leicht, übersichtlich und angenehm oder entsprechend gegenteilig beschreiben.
Service, Wartung und Support	Umfasst alle Maßnahmen, die durch den Anbieter durchgeführt werden, um die Implementierung oder den Betrieb der Lösung zu unterstützen. In einem weiteren Sinne werden der Definition auch Aussgen über die Aktualität und den Innovierungsgrad einer Lösung und insbesondere der Funktionalität zugeordnet.	[Es ist wichtig, dass der Anbieter]in regelmäßigen Abständen dementsprechend Updates anbietet und da müssen natürlich die Security-Firmen dann permanent aktiv sein. IP7 [Wir hatten] bei fast jedem Upgrade irgendwelche Schwierigkeiten. IP9 Denn wir stellen immer mehr und mehr fest, dass viele Anwender, wenn man quasi ein Update anbietet, dass viele Anwender sich schwer tun, dieses Update zu installieren, weil sie immer die Gefahr sehen, funktioniert mein System danach noch? IP7	Die Kategorie beinhaltet alle Aussagen, welche eine gewünschte oder tatsächliche Aktivitität des Anbieters bezeichnen, die eine zeitlich beständige Qualität der Kategorien Funktionalität, Interoperabilität und Benutzerfreundlichkeit vor und bei dem Betrieb der Lösung bezwecken. Hierunter fallen Aspekte zum Thema Update der Lösung und Hilfestellungen bei vor allen Dingen funktionalen Problemen.

Die folgenden Anhänge 5 bis 7 dieser Arbeit dürfen weder als Ganzes noch in Auszügen Personen außerhalb des Prüfungs- und Evaluationsverfahrens zugänglich gemacht werden, sofern keine anders lautende Genehmigung des Autors vorliegt.

Literaturverzeichnis

Baki, B./Çakar, K. (2005): Determining the ERP package-selecting criteria: the case of Turkish manufacturing companies. In: *Business Process Management Journal*.

Berger-Grabner, D. (2016): Wissenschaftliches Arbeiten in den Wirtschafts-und Sozialwissenschaften. Springer.

Bernroider, E./Koch, S. (2001): ERP selection process in midsize and large organizations. In: *Business Process Management Journal*.

Bhattacherjee, A./Hikmet, N. (2007): Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. In: *European Journal of Information Systems* 16.6, S. 725–737.

Bortz, J./Döring, N. (2006): „Qualitative Methoden". In: *Forschungsmethoden und Evaluation*. Springer, S. 295–350.

Davis, F. D. (1985): A technology acceptance model for empirically testing new end-user information systems: Theory and results. Diss. Massachusetts Institute of Technology.

– **(1989)**: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. In: *MIS Quarterly* 13.3, S. 319.

Davis, F. D./Bagozzi, R. P./Warshaw, P. R. (1989): User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. In: *Management Science* 35.8, S. 982–1003.

Dresing, T./Pehl, T. (2020): „Transkription". In: *Handbuch qualitative Forschung in der Psychologie*. Springer, S. 835–854.

Eckhardt, A./Laumer, S./Weitzel, T. (2009): Who influences whom? Analyzing workplace referents' social influence on IT adoption and non-adoption. In: *Journal of information technology* 24.1, S. 11–24.

Everdingen, Y./Waarts, E. (2003): A multi-country study of the adoption of ERP systems. In:

Flick, U. (2009): Sozialforschung: Methoden und Anwendungen: Ein Überblick für die BA-Studiengänge. In: *Ein Überblick für die BA-Studiengänge.*

– **(2011)**: Triangulation - Eine Einführung. Wiesbaden.

– **(2020)**: „Gütekriterien qualitativer Forschung". In: *Handbuch Qualitative Forschung in der Psychologie: Band 2: Designs und Verfahren*. Hrsg. von Günter Mey/Katja Mruck. Wiesbaden: Springer Fachmedien Wiesbaden, S. 247–263.

Gefen, D./Straub, D. (2000): The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption. In: *Journal of the association for Information Systems* 1.8, S. 1–30.

Gläser, J./Laudel, G. (2009): Experteninterviews und qualitative Inhaltsanalyse: als Instrumente rekonstruierender Untersuchungen. Springer-Verlag.

Hopf, C. (2016): „Soziologie und qualitative Sozialforschung". In: *Schriften zu Methodologie und Methoden qualitativer Sozialforschung*. Springer, S. 13–45.

HP Inc. (2021a): HP PCs - Set Up and Use HP Sure Admin. In: URL: `https://support.hp.com/hk-en/document/c06487900`.

HP Inc. (2021b): Infosheet - HP Sure Admin. In: URL: https://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA7-7978ENW.

– **(2021c)**: User Guide HP Sure Admin. In: S. 1–6. URL: http://h10032.www1.hp.com/ctg/Manual/c06529817.

Hussy, W./Schreier, M./Echterhoff, G. (2010): Forschungsmethoden in psychologie und sozialwissensch für bachelor. Springer-Verlag.

Illa, X. B./Franch, X./Pastor, J. A. (2000): Formalising ERP selection criteria. In: *Tenth International Workshop on Software Specification and Design. IWSSD-10 2000*, S. 115–122.

International Organization for Standardization (2011): Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models: ISO/IEC 25010:2011: Standard. Geneva, CH.

– **(2017)**: ISO/IEC/IEEE International Standard - Systems and software engineering–Vocabulary. In: *ISO/IEC/IEEE 24765:2017(E)*, S. 1–541.

Joshi, K. (1991): A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation. In: *MIS Quarterly* 15.2, S. 229–240.

Jungbauer, M. (2014): Identifikation von Nutzungstreibern und-barrieren bei Remote-Services im Aftersales-Bereich der Automobilindustrie. Diss.

Kahneman, D./Slovic, S. P./Slovic, P./Tversky, A. (1982): Judgment under uncertainty: Heuristics and biases. Cambridge university press.

Keen, P. G. W. (1981): Information systems and organizational change. In: *Communications of the ACM* 24.1, S. 24–33.

King, W. R./He, J. (2006): A meta-analysis of the technology acceptance model. In: *Information & Management* 43.6, S. 740–755.

Kollmann, T. (1998): Akzeptanz innovativer Nutzungsgüter und -systeme: Konsequenzen für die Einführung von Telekommunikations- und Multimediasystemen. Bd. 239. Neue betriebswirtschaftliche Forschung. Wiesbaden: Gabler Verlag.

Kumar, V./Maheshwari, B./Kumar, U. (2003): An investigation of critical management issues in ERP implementation: emperical evidence from Canadian organizations. In: *Technovation* 23.10, S. 793–807.

Land, F. (1992): 12 The management of change: guidelines for the successful implementation of Information Systems. In: *Creating a business-based IT strategy* 14, S. 145.

Lapointe/Rivard (2005): A Multilevel Model of Resistance to Information Technology Implementation. In: *MIS Quarterly* 29.3, S. 461.

Lee, Y./Kozar, K. A./Larsen, K. R. (2003): The Technology Acceptance Model: Past, Present, and Future. In: *Communications of the Association for Information Systems* 12.

Leitch, S./Warren, M. J. (2010): ETHICS: The past, present and future of socio-technical systems design. In: *IFIP International Conference on the History of Computing*, S. 189–197.

Lepistö, L. (2014): Taking information technology seriously: on the legitimating discourses of enterprise resource planning system adoption. In: *Journal of Management Control* 25.3-4, S. 193–219.

Leyh, C. (2016): „Critical success factors for ERP projects in small and medium-sized enterprises—the perspective of selected ERP system vendors“. In: *Multidimensional views on enterprise information systems*. Springer, S. 7–22.

Linthicum, D. S. (2000): Enterprise application integration. Addison-Wesley Professional.

Madden, T. J./Ellen, P. S./Ajzen, I. (1992): A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. In: *Personality and Social Psychology Bulletin* 18.1, S. 3–9.

Markus, M. L. (1983): Power, politics, and MIS implementation. In: *Communications of the ACM* 26.6, S. 430–444.

Mauterer, H. (2013): Der Nutzen von ERP-Systemen: Eine Analyse am Beispiel von SAP R/3. Springer-Verlag.

Mayer, H. O. (2008): Interview und schriftliche Befragung, Entwicklung, Durchführung und Auswertung, 4. In: *Auflage, München*.

Mayring, P. (2015): Qualitative Inhaltsanalyse: Grundlagen und Techniken. 12., überarb. Aufl. Weinheim/Basel: Beltz Verlag.

– **(2020)**: „Qualitative Forschungsdesigns“. In: *Handbuch Qualitative Forschung in der Psychologie*. Springer, S. 3–17.

Müller-Böling, D./Müller, M. (1986): Akzeptanzfaktoren der Bürokommunikation. R. Oldenbourg.

Pareto, V. (1912): Manuel d'économie politique. In: *Bull. Amer. Math. Soc* 18, S. 462–474.

Petra Suwalski (2020): Systemakkreditierung an Hochschulen: Anforderungen, Maßnahmen und Effekte aus der Perspektive von Hochschulakteuren. 1. Aufl. Verlag Barbara Budrich.

Pfadenhauer, M. (2009): „Das experteninterview“. In: *Qualitative Marktforschung*. Springer, S. 449–461.

Rao, S. S. (2000): Enterprise resource planning: business needs and technologies. In: *Industrial management & data systems*.

Samhan, B. u. a. (2018): Revisiting technology resistance: Current insights and future directions. In: *Australasian Journal of Information Systems* 22.

Saunders, M./Lewis, P./Thornhill, A. (2009): Research methods for business students. Pearson education.

Shehab, E. M./Sharp, M. W./Supramaniam, L./Spedding, T. A. (2004): Enterprise resource planning. In: *Business Process Management Journal* 10.4, S. 359–386.

Simon, B. (2001): Wissensmedien im Bildungssektor. Eine Akzeptanzuntersuchung an Hochschulen. Diss. Augasse 2-6, A-1090 Wien, Austria.

Themistocleous, M./Irani, Z./O'Keefe, R. M./Paul, R. (2001): ERP problems and application integration issues: An empirical survey. In: *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, S. 1–10.

Venkatesh, V./Davis, F. D. (2000): A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. In: *Management Science* 46.2, S. 186–204.

Venkatesh, V./Morris, M. G./Davis, G. B./Davis, F. D. (2003): User acceptance of information technology: Toward a unified view. In: *MIS Quarterly*, S. 425–478.

Vogelsang, K./Steinhüser, M./Hoppe, U. (2013): Theorieentwicklung in der Akzeptanzforschung: Entwicklung eines Modells auf Basis einer qualitativen Studie. In: *Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI2013) - Volume 2*. Hrsg. von Rainer Alt/Bogdan Franczyk. Bd. 27. Leipzig: Universität Leipzig, S. 1425–1439.

Erklärung

Ich versichere hiermit, dass ich meine Bachelorarbeit mit dem Thema: *Nutzen- und hemmnisorientierte Evaluation einer Client Security Lösung am Beispiel von „HP Sure Admin“* selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Tübingen, den 10. Mai 2021
(Ort, Datum)


(Unterschrift)