**ZHAW Zürcher Hochschule für Angewandte Wissenschaften**
School of Management and Law

# Bug-Bounty in Gemeinden der Deutschschweiz

## Masterthesis

| | |
|---|---|
| eingereicht im Rahmen des Studienganges | **Master of Science in Business Administration**<br>**Major Public and Nonprofit Management** |
| vorgelegt von | **Pascal Kilian Fritzenwallner** |
| Expertinnen | **Katharina Guirguis**<br>Hauptbetreuerin |
| | **Dr. Lyn Pleger**<br>Co-Betreuerin |
| Ort und Datum des Einreichens | **Winterthur, 11. Juni 2023** |

Schriftliche Arbeit verfasst an der School of Management and Law,
Zürcher Hochschule für angewandte Wissenschaften.

# Vorwort

Die vorliegende Masterarbeit *Bug-Bounty-Programme in Gemeinden der Deutschschweiz* ist das Ergebnis einer intensiven Forschungszeit und der Höhepunkt des Masterstudiums. Die wachsende Bedrohung durch Cyberangriffe und die zunehmende Notwendigkeit, digitale Systeme zu schützen, haben mich für den Themenvorschlag von meiner Co-Betreuerin, Dr. Lyn Pleger, begeistert. Als digital-affiner Verwaltungsangestelter in einer Berner Gemeinde habe ich mich spezifisch für diese Staatsebene interessiert und das Thema entsprechend ausgerichtet.

Das Hauptziel dieser Arbeit ist es, die Akzeptanz von Bug-Bounty-Programmen in Gemeinden der Deutschschweiz zu untersuchen und damit einen Beitrag zur Verbesserung der Cybersicherheit zu leisten. Die Ergebnisse der Studie sollen dazu beitragen, das Bewusstsein für die Wirkung von Bug-Bounty-Programmen zu schärfen und die Gemeinden in der Deutschschweiz zur Programmteilnahme ermutigen. Die Durchführung der Forschungsarbeit war nicht ganz ohne Herausforderungen. Im Zentrum stand die Frage, ob überhaupt genügend Personen für die quantitative Umfrage gewonnen werden konnten, da Cybersicherheit für viele Menschen ein abstraktes Thema ist und ein gewisses Verständnis erfordert. Daher bin ich allen dankbar, die ihre knappe Zeit grosszügig geteilt haben, und bedanke mich an dieser Stelle bei den Gemeinden, resp. den Teilnehmenden an der Umfrage.

Abschliessend bedanke ich mich bei allen Personen, die mich während meiner Forschungsarbeit unterstützt haben. Ein spezieller Dank gilt meiner Hauptbetreuerin, Katharina Guriguis, welche mir stets wertvolle Ratschläge und Feedback gegeben hat. Gleichzeitig danke ich meiner Ehefrau, Alina Fritzenwallner, und meiner Arbeitskollegin, Manuela Riesen, für das Lektorat. Ihre Beiträge haben wesentlich zur Qualität dieser Arbeit beigetragen.

## Management Summary

In einer Zeit, in der die digitale Transformation rasch voranschreitet und die Abhängigkeit von digitalen Systemen zunimmt, ist es von entscheidender Bedeutung, die Sicherheit dieser Systeme zu gewährleisten. Ransomware sucht automatisiert nach Einfalltoren, verschlüsselt die Systeme und fordert von den Opfern Lösegelder. Gerade die Gemeinden sind hierbei ein interessantes Ziel, da sie eine Vielzahl von persönlichen Daten bearbeiten. Gleichzeitig werden IT-Infrastrukturen häufig mittels Cloud-Dienstleistung von externen Unternehmen bezogen, wodurch die Kontrolle über die Systemsicherheit teilweise verloren geht. Ein Outsourcing der Verantwortung für Datenverluste ist jedoch nicht möglich; diese bleibt bei der Gemeinde. Daher gilt es neben dem digitalen Angebot auch die Sicherheitsmassnahmen auszubauen.

In dieser Hinsicht können Bug-Bounty-Programme eine wertvolle Ergänzung zu herkömmlichen Sicherheitsmechanismen darstellen, indem sie die Schwarmintelligenz nutzen und potenzielle Schwachstellen schneller identifizieren. In den letzten Jahren haben diese zunehmend an Bedeutung gewonnen und sie sind ein wirksames Mittel, um die Sicherheit von Software und digitaler Infrastruktur zu verbessern. Durch den Einbezug der Öffentlichkeit in den Prozess der Entdeckung von Schwachstellen und deren Behebung, haben die Organisationen Zugang zu einer breiten Basis an talentiertem Sicherheitspersonal auf der ganzen Welt. Trotzdem machen Gemeinden bisher wenig Gebrauch von dieser Massnahme. Daher soll mit der vorliegenden Arbeit erforscht werden, welche Faktoren die Gemeinden zu einer Nutzung der Bug-Bounty-Programme bewegen würden.

Infolge fehlender einschlägiger Forschungsliteratur betreffend Bug-Bounty-Programmen wurde ein Konzeptmodell auf Basis der bestehenden Literatur der allgemeinen Akzeptanz von IT-Innovationen erarbeitet. Eine wichtige Grundlage sind dabei die Diffusion of Innovation Theory, das Technology Acceptance Model sowie das Technology-Organization-Environment-Framework. Das aufge-

stellte Konzeptmodell wurde anschliessend mittels einer quantitativen Forschung überprüft. Hierzu wurde eine Umfrage bei allen Gemeinden der Deutschschweiz durchgeführt. Die gewonnenen Daten wurden analysiert und interpretiert, um die unterschiedlichen Ansichten und Wahrnehmungen der Gemeinden in Bezug auf die Bug-Bounty-Programme zu verstehen. Dabei zeigt sich, dass die Nutzungsabsicht von mehreren Faktoren der Organisation und der technischen Ausgestaltung der Massnahme abhängt.

Spezifisch lässt sich festhalten, dass die innovativen Sicherheitsmassnahmen (wie z. B. Bug-Bounty-Programme) eine geringe Komplexität aufweisen müssen, damit die Nutzungsabsicht höher ist. Einen positiven Einfluss auf die Nutzungsabsicht aus dem Blickwinkel der Technologiefaktoren haben ebenfalls der relative Vorteil (bessere Resultate als vergleichbare Massnahmen), die Kompatibilität mit den Wertevorstellungen, die Beobachtbarkeit der Resultate und die Testbarkeit vor einer definitiven Einführung. Bei den organisatorischen Faktoren der Gemeinde, welche die Massnahme einsetzt, muss insbesondere der Support durch die Exekutive, die Bereitschaft und die Expertise in Bezug auf die Informationssicherheit vorhanden sein. Im Gegenzug konnte bei der Organisationsgrösse, der Kultur und der Regulation keine signifikanten Einflüsse festgestellt werden.

Heute sind die Bug-Bounty-Programme bei den Gemeinden noch weitgehend unbekannt. Es besteht ein Informationsbedarf über den Einsatz der Programme. Damit die Gemeinden solche Programme effektiv adaptieren, sollte ein spezielles Augenmerk auf die Komplexität und den Vorteil in Bezug auf Resultat und Kosten gelegt werden. Dank der vorliegenden Arbeit konnte eine Forschungslücke betreffend die Akzeptanz von Bug-Bounty-Programmen in der öffentlichen Verwaltung geschlossen werden. Die Arbeit dient als Grundlage für weitere Forschung, damit Kausalitäten ermittelt und so verlässliche Aussagen über die Adaptionsentscheide von innovativen Massnahmen zur Steigerung der Informationssicherheit von Gemeinden getroffen werden können.

# Inhaltsverzeichnis

**ABBILDUNGSVERZEICHNIS ..... VII**
**TABELLENVERZEICHNIS ..... VII**
**ABKÜRZUNGSVERZEICHNIS ..... VIII**
**1 EINLEITUNG ..... 1**
**1.1 Ausgangslage ..... 1**
**1.2 Problemstellung und Zielsetzung ..... 4**
**1.3 Aufbau der Arbeit und methodisches Vorgehen ..... 4**
**1.4 Abgrenzung ..... 5**
**2 THEORETISCHE GRUNDLAGEN ..... 6**
**2.1 Relevanz der Informatik ..... 6**
**2.2 Betrieb der Informatikinfrastruktur ..... 7**
2.2.1 Cloud-Computing ..... 7
2.2.2 Sicherheitsaspekte im Cloud-Computing ..... 10
**2.3 Arten und Identifikation von Sicherheitslücken ..... 13**
2.3.1 Gefahren und Schäden ..... 13
2.3.2 Umgang mit Risiken ..... 15
**2.4 Bug-Bounty-Programme ..... 16**
2.4.1 Definition ..... 16
2.4.2 Kosten ..... 17
2.4.3 Einsatzbereich ..... 17
**2.5 Akzeptanz von Technologien ..... 18**
2.5.1 DOI: Diffusion of Innovation Theory ..... 18
2.5.2 TAM: Technology Acceptance Model ..... 20
2.5.3 TOE: Technology-Organization-Environment-Framework ..... 22
2.5.4 Synthetisiertes Modell und deren Einflussfaktoren ..... 23
**3 MODELL UND HYPOTHESE ..... 25**
**3.1 Forschungsfrage ..... 25**
**3.2 Konzeptmodell und Hypothesen ..... 25**
**4 FORSCHUNGSDESIGN ..... 28**
**4.1 Methodisches Vorgehen ..... 28**
**4.2 Stichprobe ..... 29**
**4.3 Datenerhebung und Fragebogen ..... 29**
4.3.1 Aufbau ..... 29
4.3.2 Operationalisierung ..... 29
4.3.3 Pretest ..... 30
**4.4 Datenauswertung ..... 30**
**4.5 Gütekriterien ..... 31**
**5 RESULTATE ..... 32**
**5.1 Beschreibung der Stichprobe ..... 32**
Gruppenzusammensetzung ..... 34
**5.2 Faktoren Organisation ..... 35**
5.2.1 Support der Exekutive ..... 35
5.2.2 Organisationsgrösse ..... 36
5.2.3 IS-Expertise ..... 36
5.2.4 IS-Bereitschaft ..... 36
5.2.5 IS-Kultur ..... 37

5.2.6 Zusammenfassung der Faktoren Organisation ..... 37
**5.3 Faktoren Technologie ..... 37**
5.3.1 Relativer Vorteil ..... 38
5.3.2 Komplexität ..... 39
5.3.3 Kompatibilität ..... 39
5.3.4 Beobachtbarkeit ..... 39
5.3.5 Testbarkeit ..... 39
5.3.6 Zusammenfassung der Faktoren Technologie ..... 39
**5.4 Faktoren Umwelt ..... 40**
5.4.1 Regulation Wichtigkeit ..... 40
5.4.2 Regulation Nützlichkeit ..... 41
5.4.3 Regulation Kostensenkung ..... 41
5.4.4 Zusammenfassung der Faktoren Umwelt ..... 41
**5.5 Relevanz der Faktoren ..... 42**
**5.6 Erfüllung der Faktoren von Bug-Bounty-Programmen ..... 43**
**5.7 Weitere Resultate ..... 45**
5.7.1 Bekanntheit und Nutzung ..... 45
5.7.2 Verantwortungsbewusstsein ..... 46
**6 DISKUSSION UND WÜRDIGUNG ..... 47**
**6.1 Faktoren Organisation ..... 47**
**6.2 Faktoren Technologie ..... 48**
**6.3 Faktoren Umwelt ..... 50**
**7 SCHLUSSFOLGERUNGEN UND IMPLIKATIONEN ..... 51**
**7.1 Implikationen für die Forschung ..... 52**
**7.2 Implikationen für die Praxis ..... 53**
**7.3 Limitationen und weitere Forschung ..... 54**
**8 LITERATURVERZEICHNIS ..... 55**
**9 ANHANG ..... 61**
**9.1 Fragebogen ..... 61**
**9.2 Operationalisierung unabhängige Variablen ..... 70**

# Abbildungsverzeichnis

Abbildung 1: Digitalisierungsstrategien der Kantone in der Schweiz ..... 1
Abbildung 2: Entwicklung der Teleheimarbeit in der Schweiz ..... 3
Abbildung 3: Betriebsmodelle Cloud-Computing ..... 9
Abbildung 4: Einfluss von Cloud-Betriebsmodellen ..... 10
Abbildung 5: Kategorisierung von Cyber-Risiken ..... 14
Abbildung 6: Technologieakzeptanzmodell ..... 21
Abbildung 7: TOE-Framework ..... 22
Abbildung 8: Vorgeschlagenes Modell zur Einführung von Informationssicherheitsinnovationen in Organisationen ..... 24
Abbildung 9: Konzeptmodell ..... 26
Abbildung 10: Karte der teilnehmenden Gemeinden ..... 32
Abbildung 11: Relevanz der Faktoren zur Adaption von innovativen IS-Massnahmen ..... 42
Abbildung 12: Bekanntheit von BBP nach Gemeindetypologie ..... 45
Abbildung 13: Umgang mit Hypothesen ..... 51

# Tabellenverzeichnis

Tabelle 1: Service-Levels in der Cloud-Architektur ..... 8
Tabelle 2: Grösste Bedrohungen im Cloud-Computing ..... 12
Tabelle 3: Umgang mit Cyber-Risiken ..... 15
Tabelle 4: Beschreibung der Stichprobe ..... 33
Tabelle 5: Zusammensetzung der Untersuchungsgruppen ..... 34
Tabelle 6: Deskriptive Statistik der Faktoren Organisation ..... 35
Tabelle 7: Teststatistik Mann-Whitney-U-Test, Faktoren Organisation ..... 37
Tabelle 8: Deskriptive Statistik der Faktoren Technologie ..... 38
Tabelle 9: Teststatistik Mann-Whitney-U-Test, Faktoren Technologie ..... 40
Tabelle 10: Deskriptive Statistik der Faktoren Umwelt ..... 40
Tabelle 11: Teststatistik Mann-Whitney-U-Test, Faktoren Umwelt ..... 41
Tabelle 12: Relevanz der Faktoren zur Adaption von innovativen IS-Massnahmen ..... 43
Tabelle 13: Deskriptive Statistik, Faktoren BBP ..... 43
Tabelle 14: Teststatistik Mann-Whitney-U-Test, Faktoren BBP ..... 44
Tabelle 15: Ergebnisse Faktor Verantwortung ..... 46

# Abkürzungsverzeichnis

| | |
|---|---|
| BBP | Bug-Bounty-Programm |
| BSI | Bundesamt für Sicherheit in der Informationstechnik (Deutschland) |
| CI | Konfidenzintervall |
| DOI | Diffusion of Innovation Theory |
| ENISA | Agentur der Europäischen Union für Cybersicherheit |
| IS | Informationssicherheit |
| NCSC | Nationales Zentrum für Cybersicherheit (Schweiz) |
| NIST | National Institute of Standards and Technology (USA) |
| TAM | Technology Acceptance Model |
| TOE | Technology-Organization-Environment Framework |
| TPB | Theory of planned behaviour |

# 1 Einleitung

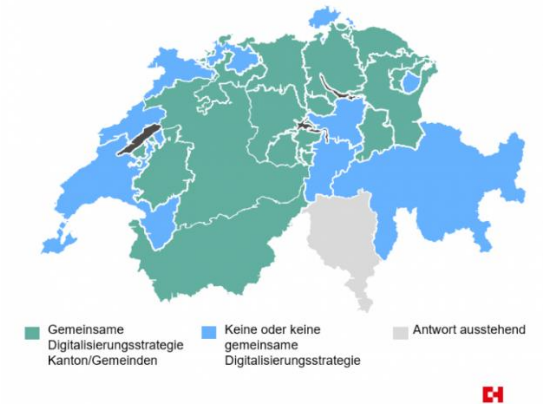
## 1.1 Ausgangslage

Sei es der elektronische Umzug oder das Einreichen eines Baudossiers; die Digitalisierung schreitet in der öffentlichen Verwaltung auf allen Staatsebenen voran. Der Kanton Bern hat beispielsweise per 1. März 2023 mittels Gesetz und Verordnung über die digitale Verwaltung den Grundsatz «digital first» beschlossen, so dass künftig Bevölkerung, Wirtschaft und Behörden untereinander digital kommunizieren können (Staatskanzlei Kanton Bern, 2023a). In seiner Vision hat sich der Kanton Bern insbesondere drei Leitlinien gesetzt:

- Elektronische Abwicklung sämtlicher Geschäfte durch die Bevölkerung;
- Moderne und elektronische Geschäftsprozesse innerhalb der Verwaltung;
- Standardmässige elektronische Geschäftsabwicklung durch die Wirtschaft (Staatskanzlei Kanton Bern, 2023b, S. 13)

Nicht nur der Kanton Bern setzt in seiner Strategie vollständig auf die Digitalisierung. In nahezu allen Kantonen der Schweiz ist eine Digitalisierungs-, E-Government- oder Informatikstrategie umgesetzt oder kurz vor der Umsetzung (Digitale Verwaltung Schweiz, 2023, S. 1). Häufig liegt der Fokus aber nicht isoliert auf dem Kanton, sondern auch die Gemeinden werden in die Strategie miteinbezogen (gemäss Abbildung 1).

**Abbildung 1: Digitalisierungsstrategien der Kantone in der Schweiz**

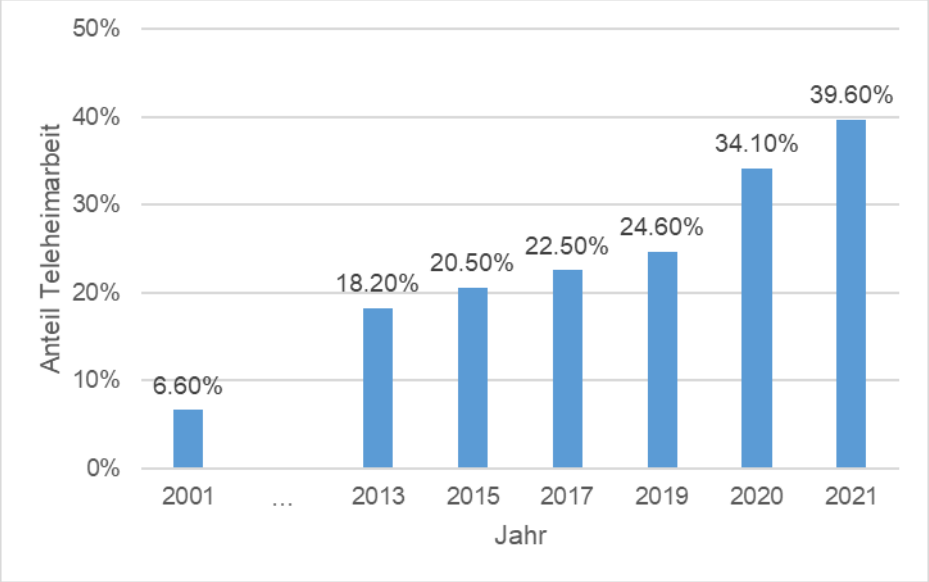



*Anmerkung:* Abbildung von Digitale Verwaltung Schweiz (2023, S. 4).

Gleichzeitig hat die Schweiz einen hohen Aufholbedarf bei der Digitalisierung. Im europäischen Vergleich befindet sich die Schweiz zwar mit Rang 15 von 35 noch im Mittelfeld; primär aber dank hohen Werten in den Bereichen Humankapital und Telekominfrastruktur. Wird nur der Online-Service-Index der Verwaltung betrachtet, landet die Schweiz noch auf Rang 26 (United Nations, 2022, S. 72). Ein ähnliches Bild zeigt sich bei der Informationssicherheit. Hier belegt die Schweiz im europäischen Vergleich ebenfalls Rang 26 (International Telecommunication Union, 2021, S. 30). Speziell im Rechtswesen, also der Gesetzgebung betreffend Cybersicherheit, Datenschutz und kritischer Infrastruktur, sieht der Bericht Aufholbedarf für die Schweiz (International Telecommunication Union, 2021, S. 127).

Neben der tiefen Rangierung der Schweiz im internationalen Vergleich, entsteht Druck aus der Bevölkerung auf die Kommunen. Gemäss der nationalen E-Government-Studie 2021 denken 41 % der befragten Privatpersonen, dass das Online-Angebot der Wohngemeinde eher bis sehr stark ausgebaut werden sollte (Buess et al., 2022, S. 83). Die Kundinnen und Kunden wünschen sich also vermehrt digitale Kontaktpunkte zur kommunalen Verwaltung. Neben der Bevölkerung und der Wirtschaft sind weiter die Angestellten eine wichtige Anspruchsgruppe. Auch hier zeigt sich ein Bedürfnis nach Digitalisierung. Der Anteil an Teleheimarbeit (definiert als «Internetnutzung für den Datenaustausch mit dem Arbeit- oder Auftraggeber») ist gemäss Bundesamt für Statistik (BFS, 2022) in den vergangenen Jahren kontinuierlich angestiegen und betrug zuletzt 39.60 % aller Erwerbstätigen (siehe Abbildung 2).

**Abbildung 2: Entwicklung der Teleheimarbeit in der Schweiz**




*Anmerkung:* Eigene Darstellung nach Bundesamt für Statistik (2022b).

Kundinnen und Kunden erwarten also zunehmend digitale Dienstleistungen und die Mitarbeitenden benötigen für das Homeoffice Informatik-Ressourcen. Hierfür wird im Hintergrund eine entsprechende Infrastruktur vorausgesetzt. Dabei stehen die Behörden vor der klassischen Fragestellung, ob die Leistung der Informatik selbständig oder durch eine externe Stelle erbracht werden soll. Unabhängig von der gewählten Variante ist insbesondere dem Datenschutz und der Datensicherheit Rechnung zu tragen.

Das revidierte Datenschutzgesetz der Schweiz tritt am 1. September 2023 auf Bundesebene in Kraft. Dieses hat zwar kaum direkte Auswirkungen auf Gemeinden, da diese dem Bundesrecht nur unterstellt sind, sofern sie als Private handeln und nicht als öffentliche Organe (Regierungsrat Kanton Basel-Stadt, 2021, S. 1). Wie der Regierungsrat des Kantons Zürich (2021, S. 1) in seiner Stellungnahme zum neuen Datenschutzgesetz jedoch festhält, kann dieses als Orientierungshilfe dienen, um kantonales und kommunales Recht anzupassen. Durch die erwartete Angleichung der kantonalen Datenschutzgesetze werden somit zukünftig auch die Gemeinden in die Pflicht genommen, da diese eine Vielzahl von persönlichen Daten verwalten. Zudem hat die Vergangenheit gezeigt, dass Gemeinden nicht vor kriminellen Cyberattacken, wie Rolle VD im

Mai 2021 (Anz, 2021), oder Datenverlusten, wie Landiswil BE im April 2021 (Bundi, 2021), gefeit sind. Eine Möglichkeit, um die Sicherheit der eingesetzten Systeme zu prüfen, sind Bug-Bounty-Programme. Nachdem solche Programme bei den globalen Digitalunternehmen wie Google (Paresh, 2017) und Microsoft (Microsoft Security Response Center, 2017) bereits seit mehreren Jahren eingesetzt werden, wurde im Jahr 2021 auch in der Schweizer Bundesverwaltung ein entsprechendes Pilotprojekt gestartet (NCSC, 2021, S. 3). Vom Einsatz solcher Programme in Schweizer Gemeinden ist bisher wenig bekannt.

## 1.2 Problemstellung und Zielsetzung

Im Gegenzug zur Privatwirtschaft und der Bundesverwaltung sind Gemeinden bisher wenig von Bug-Bounty-Programmen berührt. Im Rahmen der Masterarbeit sollen die Gründe hierfür evaluiert werden. Gleichzeitig soll eine erste Bestandsaufnahme über die Organisation der Informatik (Out- oder Insourcing) in Deutschschweizer Gemeinden erhoben werden.

## 1.3 Aufbau der Arbeit und methodisches Vorgehen

Um die vorgängig erwähnte Zielsetzung zu erreichen, wird in Kapitel 2 eine Bestandesaufnahme über den Stand des aktuellen Wissens in verschiedenen Themengebieten erstellt. Diese umfasst insbesondere die Relevanz der Informatik sowie deren Betriebsmöglichkeiten, die Risiken und deren Bewältigung, als auch Bug-Bounty-Programme und den Forschungsstand betreffend die Akzeptanz von Technologien. In Kapitel 3 wird aus den theoretischen Grundlagen die Forschungsfrage sowie das Konzeptmodell mit verschiedenen Hypothesen abgeleitet. Diese Hypothesen werden mittels einer quantitativen Forschung überprüft, deren Vorgehen (Kapitel 4) und Resultate (Kapitel 5) entsprechend präsentiert werden. Zum Schluss werden die Resultate in Kapitel 6 mit den aktuellen Erkenntnissen verbunden und diskutiert, um daraus mögliche Handlungsoptionen für Forschung und Praxis abzuleiten (Kapitel 7).

Da bisher keine einschlägige Forschung zur Akzeptanz von Bug-Bounty-Programmen in Kommunen oder der öffentlichen Verwaltung allgemein bestehen, werden bestehende Theorien zur Akzeptanz von Technologien hinzugezogen. Im Speziellen werden folgende Modelle berücksichtigt:

- DOI: Diffusion of Innovation Theory von Rogers, 1983
- TAM: Technology Acceptance Model von Davis, 1989
- TOE: Technology–Organization–Environment framework von Tornatzky und Fleischer, 1990

Im Rahmen der schriftlichen Arbeit wird die Eignung der Akzeptanzmodelle für die Adaption von Bug-Bounty-Programmen geprüft und ein entsprechendes Konzeptmodell entwickelt. Als Grundlage dient spezifisch das Modell zur Adaption von Cybersecurity-Innovationen durch Organisationen von Hameed und Arachchilage (2017). Das Modell wird mittels einer quantitativen Umfrage bei den Deutschschweizer Gemeinden angewendet, um die Einflussfaktoren zu bestimmen und Handlungsoptionen abzuleiten.

## 1.4 Abgrenzung

Als Deutschschweizer Gemeinden werden alle Gemeinden aus nachfolgenden Kantonen definiert: Aargau, Appenzell Ausserrhoden, Appenzell Innerrhoden, Basel-Landschaft, Basel-Stadt, Glarus, Luzern, Nidwalden, Obwalden, Schaffhausen, Schwyz, Solothurn, St. Gallen, Thurgau, Uri, Zug und Zürich. Bei den zwei- oder mehrsprachigen Kantonen Bern, Freiburg, Graubünden und Wallis wurde die Sprachzuordnung nach Bundesamt für Statistik (2016) berücksichtigt. Daraus resultiert ein Umfang von 1’382 Gemeinden.

# 2 Theoretische Grundlagen

In den nachfolgenden Kapiteln werden die theoretischen Grundlagen vorgestellt. Dabei wird zu Beginn eine Einordnung der Relevanz der Informatik vorgenommen und verschiedene Betriebsstrukturen evaluiert. Anschliessend folgt eine Betrachtung der aktuellen Bedrohungen für die Informationssicherheit und wie diesen begegnet werden kann, insbesondere mittels Bug-Bounty-Programmen. Zum Abschluss dieses Kapitels wird der aktuelle Stand der Forschung in Bezug auf die Akzeptanz von Technologien dargelegt, welche die Grundlage für das Konzeptmodell bilden.

## 2.1 Relevanz der Informatik

Die Digitalisierung durchdringt sämtliche Bereiche der Gesellschaft und auch immer stärker die öffentliche Verwaltung. So hat der Schweizer Bundesrat in seiner Agenda für die Legislatur 2019 – 2023 die Nutzung der Chancen aus der Digitalisierung als eine von drei Leitlinien definiert (Schweizer Bundesrat, 2020, S. 1833f.). Von diesen Leitlinien ausgehend wurden konkrete Ziele zur Digitalisierung abgeleitet. Der Bund soll seine staatlichen Leistungen möglichst digital anbieten (Schweizer Bundesrat, 2020, S. 1835) und die Investitionen in Informations- und Kommunikationstechnologien soll dank guter Rahmenbedingungen erhöht werden (Schweizer Bundesrat, 2020, S. 1845). Das Controlling der vorangehenden Legislaturzielen zwischen 2018 und 2021 zeigt, dass bei der Nutzung von digitalen Kontaktmöglichkeiten Fortschritte erzielt wurden. Der persönliche Kontakt am Schalter und der briefliche Kontakt von Privatpersonen sind rückläufig, während sich die Nutzung von elektronischen Behördenportalen erhöht (Buess et al., 2022, S. 18). Dieser Trend widerspiegelt sich ebenfalls auf der lokalen Ebene (Buess et al., 2022, S. 20) und zeigt die Relevanz der Informatik auf allen Staatsebenen.

Um die angestrebte Digitalisierung des öffentlichen Sektors umzusetzen, werden entsprechende Ressourcen wie Rechenleistung oder Speicherkapazitäten benötigt. Deren Entwicklung zeigt sich exemplarisch an den Investitionen der Gemeinden des Kantons Bern, welche in den Jahren 2017 bis 2021 gemeinsam jährlich durchschnittlich CHF 18.4 Mio. in Software investiert haben (Finanzdirektion Kanton Bern, 2021b). Im gleichen Zeitraum haben sich die jährlichen Ausgaben für den Unterhalt der Hardware um 11 % erhöht (Finanzdirektion Kanton Bern, 2021a). Dieses Ausgabenwachstum zeigt die zunehmende Relevanz, respektive den zunehmenden Bedarf, der Informatikmittel in Gemeinden.

## 2.2 Betrieb der Informatikinfrastruktur

Trotz der Investitionsbemühungen der Gemeinden, scheint dies noch nicht zu genügen. So sehen 18.2 % der Gemeinden ihre Leistungsgrenze erreicht, um die Informatik für die Gemeindeverwaltung bereitzustellen (Steiner et al., 2021, S. 18). Den Gemeinden steht es offen, ob sie die Informatikdienstleistungen selbst bereitstellen oder mit externen Partnern zusammenarbeiten. 27.6 % der Gemeinden nutzen diese Möglichkeit und arbeiten mit privaten Unternehmen zusammen, um die Informatikaufgaben der Gemeindeverwaltung zu bewältigen (Steiner et al., 2021, S. 124f.) Dabei scheint die Grösse der Gemeinde einen Einfluss zu haben, da primär grössere Gemeinden die Informatik intern bereitstellen (Steiner et al., 2021, S. 127). Dies lässt sich durch die Grundannahme begründen, dass in grösseren Organisationen sowohl die Spezialisierung wie auch die Professionalisierung zunehmen (Jungbauer-Gans, 2016, S. 137).

### 2.2.1 Cloud-Computing

Neben dem selbständigen Betrieb der IT-Infrastruktur besteht die Möglichkeit, die gesamten Informatikprozesse oder Teile davon auszulagern. Beim Gedanken an Auslagerung von Informatikleistungen fällt schnell der Begriff «Cloud-Computing». Dessen genaue Definition gestaltet sich hingegen schwierig, da eine Vielzahl von verschiedenen Ausprägungen besteht. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) referenziert bei seiner Definition auf die US-amerikanischen Standardisierungsstelle National Institute of

Standards and Technology (NIST) wie auch die Agentur der Europäischen Union für Cybersicherheit (ENISA) und definiert Cloud-Computing wie folgt:

> *Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschliesslich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software* (BSI, 2012, S. 15f.).

Das Cloud-Computing stellt demnach eine Variante der Auslagerung dar, bei welcher die Infrastruktur nicht exklusiv einem Kunden zur Verfügung steht (keine Single Tenant Architektur) und die Dienstleistungen dynamisch den Bedürfnissen angepasst werden können (BSI, 2012, S. 18f.). Wie die obenstehende Definition impliziert, bestehen beim Cloud-Computing verschiedene Dienstleistungsebenen, respektive Service-Levels. Klassischerweise werden hier drei Levels gemäss Tabelle 1 unterschieden.

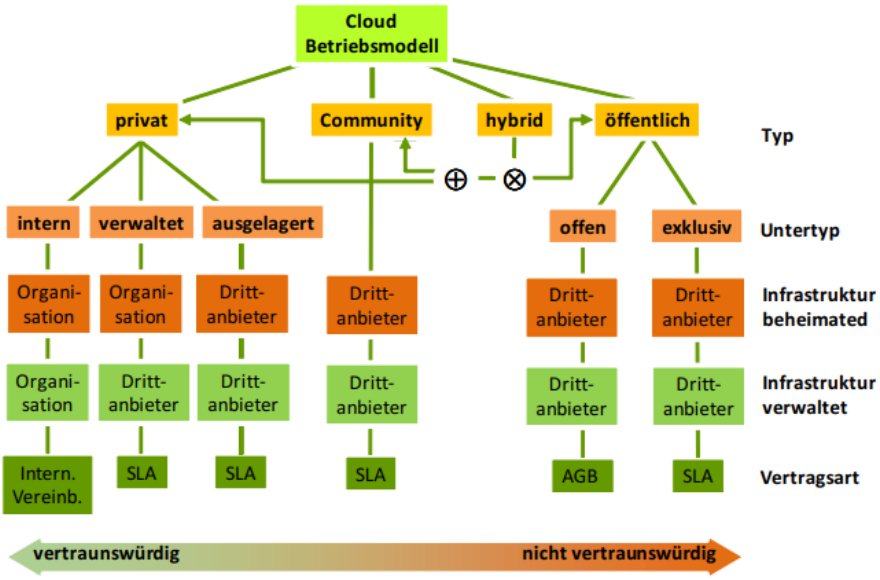
**Tabelle 1: Service-Levels in der Cloud-Architektur**

| **Service-Level** | **Merkmale** |
|---|---|
| SaaS: Software as a Service | Bereitstellung einer Applikation zur direkten Ausführung via Internet. |
| PaaS: Platform as a Service | Bereitstellung einer Plattform zur Entwicklung und Ausführung von eigenen Programmen. |
| IaaS: Infrastructure as a Service | Bereitstellung von Infrastrukturbestandteilen wie z. B. Speicherkapazität oder Rechenleistung. |

*Anmerkung:* Eigene Darstellung nach Mell und Grace (2011, S. 2f.) sowie Deussen et al. (2010, S. 16ff.)

Das Cloud-Computing kann sich somit auf einzelnen Applikationen (z. B. die Software der Einwohnerkontrolle) und die dazu notwendige Basisinfrastruktur beziehen oder es werden Infrastrukturkomponenten (IaaS) bereitgestellt, worauf die Applikationen betrieben werden. Entsprechend der gewählten Variante sind die Einflussmöglichkeiten für die Gemeinde begrenzt. Neben den Dienstleistungsebenen unterscheiden Mell und Grace (2011, S. 3) das Cloud-Computing in die vier Bereitstellungsmodelle Private Cloud, Public Cloud, Community Cloud und Hybrid Cloud. Während die Private Cloud durch eine Organisation exklusiv genutzt wird, werden die anderen durch mehrere Organisationen parallel genutzt. Abbildung 3 zeigt die wesentlichen Unterschiede der vier Modelle auf und nimmt gleichzeitig eine Beurteilung der Vertrauenswürdigkeit vor, welche mit zunehmender öffentlicher Nutzung sinkt (Deussen et al., 2010, S. 21).

**Abbildung 3: Betriebsmodelle Cloud-Computing**




*Anmerkung:* Abbildung von Deussen et al. (2010, S. 21)

Während die Private Cloud als einzige Variante vollständig durch die Organisation selbst bereitgestellt werden kann (interne Private Cloud), besteht bei allen anderen Varianten eine Verbindung zu Drittparteien bei der Infrastrukturverwaltung und oder der physischen Infrastrukturbereitstellung (Deussen et al., 2010, S. 21). Hierdurch sinken die Einflussnahme und die Kontrollmöglichkeiten der Gemeinde als Auftraggeberin, was schlussendlich zu einer Reduktion der Vertrauenswürdigkeit führt (Deussen et al., 2010, S. 21).

Eine Mischform im Sinne einer eingeschränkten Public Cloud ist die Community Cloud, bei welcher sich Institutionen mit ähnlichen Absichten (z. B. verschiedenen Gemeinden) zusammenschliessen und die Infrastruktur durch eine Organisation (eine der beteiligten Gemeinden oder eine Drittfirma) verwalten lassen (Mell & Grance, 2011, S. 3). Im Vergleich zu öffentlichen Cloudlösungen besteht ein höheres Vertrauen, da die Partnerorganisation ein gleiches Ziel verfolgt wie die auftraggebende Partei.

### 2.2.2 Sicherheitsaspekte im Cloud-Computing

Der Einsatz von Cloud-Computing führt zwangsläufig einem Kontrollverlust durch die auftraggebende Organisation, da sicherheitsrelevante Aspekte nicht mehr selbständig gesteuert werden können (Adelmeyer et al., 2018, S. 7).

Schürmann (2018, S. 55) hält hierzu fest, dass die Wahl des Betriebsmodells (vergleiche Abbildung 3 oben) einen Einfluss auf die drei Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) hat. Bei hybriden oder öffentlichen Cloud-Lösungen zeigt sich nach Abbildung 4, dass insbesondere die Vertraulichkeit wie auch die Integrität gefährdet sind. Daraus lässt sich ein Schutzbedarf ableiten.

**Abbildung 4: Einfluss von Cloud-Betriebsmodellen**

| | Private Cloud | Hybrid Cloud | Public Cloud |
|---|---|---|---|
| Vertraulichkeit | hoch, Daten bleiben im Unternehmen | gefährdet, Daten teilweise außerhalb des Unternehmens | gefährdet, Daten außerhalb des Unternehmens |
| Integrität | hoch, Daten auf eigenen Systemen | gefährdet, Daten teilweise auf Systemen Dritter | gefährdet, Daten auf Systemen Dritter |
| Verfügbarkeit | schwere Lokalisierung, hohe Verfügbarkeit | schwierigste Lokalisierung, teilweise Abhängigkeit von externer Verfügbarkeit | schwere Lokalisierung, Abhängigkeit von externer Verfügbarkeit |

*Anmerkung:* Abbildung von Schürmann (2018, S. 55, in Anlehnung an Hansen, 2009)

Die grössten wahrgenommenen Bedrohungen für Cloud-Services sind gemäss Studie der Cloud Security Alliance (2022, S. 8) vielfältig und in der Tabelle 2 unten mit den betroffenen Servicemodellen und Verantwortlichkeiten umschrieben. Dabei ist auffällig, dass trotz Outsourcing an eine Drittpartei, die Verantwortung bei allen möglichen Bedrohungen vollständig oder zumindest teilweise beim Kunden liegt und die Bedrohungen zumeist unabhängig des Servicemodells bestehen. Das Auslagern der Informatik führt demnach nicht zu einem Transfer der Verantwortung. Dies bestätig das Nationale Zentrum für Cybersicherheit (NCSC) der Schweiz, indem es bei seinen Empfehlungen für Behörden festhält: *Die Verantwortung für die Cybersicherheit liegt immer bei der Behörde!* (NCSC, 2022c).

Neben den erwähnten Sicherheitsrisiken gilt es hervorzuheben, dass Cloud-Computing die Sicherheit auch erhöhen kann. Gemäss ENISA (2009, S. 17) profitieren Cloud-Lösungen insbesondere von Skaleneffekten. So wird beispielsweise die Redundanz und somit die Ausfallsicherheit dank der Verteilung auf mehrere Standorte erhöht, während gleichzeitig vermehrt spezialisierte Personen für das Sicherheitsmanagement angestellt werden können (ENISA, 2009, S. 17). Weiter ist die Sicherheit für Cloud-Anbieter ein zwingendes Merkmal, da die Kundinnen und Kunden ihren Kaufentscheid davon abhängig machen – dies führt zu einem höheren Engagement der Provider im Bereich der Sicherheit (ENISA, 2009, S. 17f.).

**Tabelle 2: Grösste Bedrohungen im Cloud-Computing**

| **Bedrohung** | **Verantwortliche Stelle** | **Betroffene Servicemodelle** |
|---|---|---|
| Unzureichende Identitäts-, Berechtigungs-, Zugangs- und Schlüsselverwaltung | Kunde | SaaS, Paas, IaaS |
| Unsichere Schnittstellen und APIs | Kunde und Cloud-Anbieter einzeln | SaaS, Paas, IaaS |
| Fehlkonfiguration und unzureichende Änderungskontrolle | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Fehlende Cloud-Sicherheitsarchitektur und -strategie | Kunde | SaaS, Paas, IaaS |
| Unsichere Software-Entwicklung | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Unsichere Ressourcen von Drittanbietern | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Systemschwachstellen | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Unbeabsichtigte Offenlegung von Cloud-Daten | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Fehlkonfiguration und Ausnutzung von Serverless und Container Workloads | Kunde und Cloud-Anbieter geteilt | Paas, IaaS |
| Organisierte Kriminalität/Hacker/APT | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |
| Exfiltration von Cloud-Speicherdaten | Kunde und Cloud-Anbieter geteilt | SaaS, Paas, IaaS |

*Anmerkung:* Eigene Darstellung nach Cloud Security Alliance (2022, S. 8ff.)

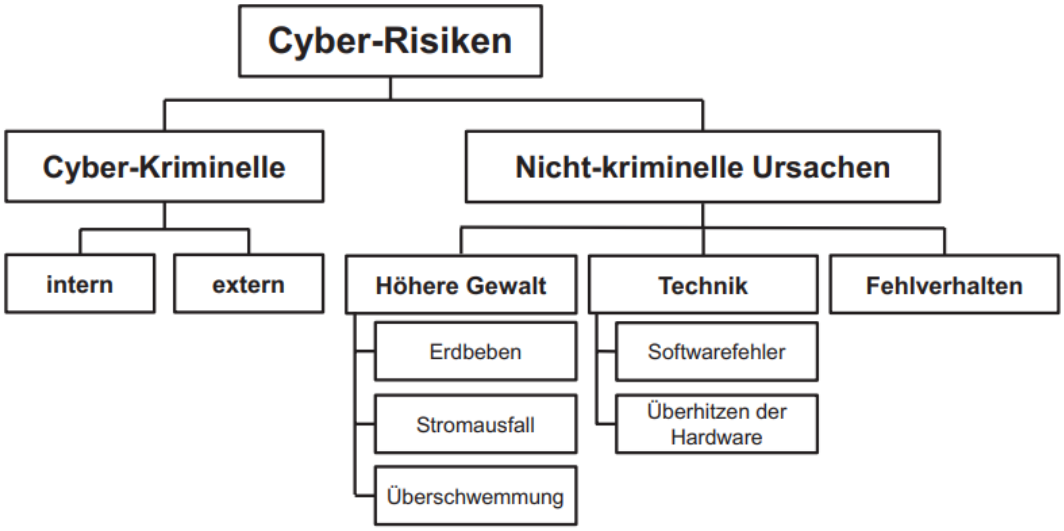
## 2.3 Arten und Identifikation von Sicherheitslücken

Neben den Cloud-spezifischen Sicherheitsbedenken gilt es, die Informationssicherheit an sich zu betrachten. Hierbei werden zumeist die Ziele der Vertraulichkeit, der Integrität, der Authentizität und der Verfügbarkeit gefährdet (Königs, 2017, S. 159). Gleichzeitig ist die Gewährleistung der Datensicherheit ein relevanter Aspekt, da in der nationalen E-Government-Studie 2021 44 % der Befragten angaben, dass das fehlende Vertrauen in den Datenschutz / die Datensicherheit, die Nutzung von E-Government-Angeboten erschwere (Buess et al., 2022, S. 29). Der Trend ist im Vergleich zu 2018 zwar rückläufig, jedoch weiterhin auf Platz 2 der grössten Hindernisse. Gleichzeitig nehmen die gemeldeten Cybervorfälle beim nationalen Zentrum für Cybersicherheit (NCSC) zu und umfassten im ersten Halbjahr 2022 insgesamt 17'186 Meldungen (NCSC, 2022a, S. 14). Nachfolgend werden die verbreitetsten Gefahren und Möglichkeiten zur Identifikation von Sicherheitslücken vorgestellt.

### 2.3.1 Gefahren und Schäden

Wie die Kategorisierung in der untenstehenden Abbildung 5 zeigt, können Gefahren und Schäden in Bezug auf die Informationssicherheit aus kriminellen wie auch nicht kriminellen Ursachen entstehen (Walz et al., 2020, S. 452). Meist werden bei Angriffen auf die Informationssicherheit organisatorische und/oder technische Schwachstellen der IT-Systeme ausgenutzt (Königs, 2017, S. 417). Die Motivation für Cyberangriffe ist vielfältig. So können es klassische kriminelle Handlungen wie Diebstahl oder Erpressung mit dem Ziel einer finanziellen Bereicherung sein oder aber auch weiterführende Motive wie Sabotage, Spionage, Desinformation oder kriegerische Handlungen sind möglich (Bundesamt für Bevölkerungsschutz, 2020, S. 1).

**Abbildung 5: Kategorisierung von Cyber-Risiken**




*Anmerkung:* Darstellung von Walz et al. (2020, S. 452)

Als akuteste Bedrohung gilt weiterhin das kriminelle Risiko der Ransomware (NCSC, 2022a, S. 24). Dabei handelt es sich um eine Art Erpressung, indem die Daten auf einem Computer verschlüsselt und erst gegen Bezahlung eines Lösegeldes wieder entsperrt werden (NCSC, 2022d). Eine Datenverletzung infolge eines Ransomware-Angriffs verursacht Kosten von durchschnittlich USD 4.54 Mio., exkl. der Lösegeldzahlungen (IBM, 2022, S. 6). Dabei wurden insbesondere die Kosten für die Erkennung und die Eskalation, die Benachrichtigung der Betroffenen und Dritten, die eigentliche Reaktion auf den Vorfall sowie die Verluste aus dem entgangenen Geschäft inkl. Reputationsverluste berücksichtigt (IBM, 2022, S. 54).

Neben der Bedrohung durch Ransomware bestehen weitere diverse Risiken für die Informationssicherheit von Gemeinden. So zählen insbesondere E-Banking-Trojaner (getarnte Schadsoftware), Phishing (Erbeuten von Passwörtern), DDoS-Attacken (Überlastung der Systeme mittels einer Vielzahl von Anfragen) oder Fernzugriffe (meist zusammen mit Phishing oder über veraltete Netzwerkkomponenten) zu den häufigsten Gefahren für Gemeinden (Kantonspolizei Bern et al., o. J., S. 6).

### 2.3.2 Umgang mit Risiken

Risken betreffend die Informationssicherheit können grundsätzlich im gleichen Prozess wie andere Unternehmensrisiken behandelt werden, wenn auch mit teilweise anderen Identifikations- und Beurteilungsmethoden (Hunziker et al., 2022, S. 38). Auf Basis der übergeordneten Risikostrategie folgt die Risikoidentifikation, Risikobewertung sowie Risikoaggregation und abschliessend die Risikosteuerung (Rohlfs & Mahnke, 2020, S. 9). Bei der Risikosteuerung stehen den Organisationen klassischerweise die Optionen der Vermeidung (Reduktion der Eintrittswahrscheinlichkeit), der Verminderung (Reduktion des Schadensausmasses), des Transfers (Überwälzung auf andere Organisation) oder die Akzeptanz zur Verfügung (Skorna & Nießen, 2020, S. 58ff.). Diese Optionen stehen der öffentlichen Hand auch im Rahmen der Informationssicherheit zur Verfügung, wie dies Tabelle 3 mit konkreten Massnahmen impliziert.

**Tabelle 3: Umgang mit Cyber-Risiken**

| Kategorie | Massnahmen |
|---|---|
| Vermeidung | Anwendung von IT-Sicherheitsstandards<br>(z. B. Virenschutz, Backups, Firewall, …) |
| | Kompetenz der Belegschaft<br>(z. B. Sensibilisierung, Schulung, Whistle-Blowing-Tools) |
| | Organisatorische Massnahmen<br>(z. B. Zugriffsbeschränkung und -kontrollen) |
| Verminderung | Schnelle Reaktionszeit (Organisation) |
| | Geregelte Abläufe und Zuständigkeiten (Organisation) |
| Transfer | Versicherungen |
| Akzeptanz | Tragen der Risiken |

*Anmerkung:* Eigene Darstellung nach Walz (2020, S. 462ff.)

Damit die Risiken gesteuert werden können, bedarf es einer vorgängigen Identifikation der Sicherheitslücken. Auf der technischen Ebene können hierzu beispielsweise Schwachstellen-Scanner oder Penetrationstests eingesetzt werden

(Königs, 2017, S. 418). Bei einem Penetrationstest wird ein Dienstleistungsunternehmen beauftragt, die IT-Infrastruktur in einem definierten Szenario anzugreifen (Schläger & Thode, 2022, S. 677). Dabei liefert der Penetrationstest eine Momentaufnahme des Sicherheitszustandes, weshalb dieser mindestens alle zwei Jahre wiederholt werden sollte (Schläger & Thode, 2022, S. 681).

## 2.4 Bug-Bounty-Programme

Neben den erwähnten Methoden zur Identifikation von Schwachstellen in der IT-Infrastruktur, werden in der Wirtschaft und der öffentlichen Verwaltung vermehrt Bug-Bounty-Programme (BBP) lanciert. Diese werden nachfolgend genauer erläutert.

### 2.4.1 Definition

Das NCSC (2022b, S. 3) beschreibt die Bug-Bounty-Programme wie folgt:

> *Bug-Bounty-Programme dienen dazu, in Zusammenarbeit mit ethischen Hackern allfällige Verwundbarkeiten in IT-Systemen und in Anwendungen zu identifizieren, zu dokumentieren und zu beheben. Die ethischen Hacker nutzen eigene Methoden, die erlauben, Schwachstellen zu identifizieren, die mit klassischen Penetrationstests oder Security Reviews nicht immer gefunden werden können.*

Ethische Hacker sind dabei IT-Fachpersonen, welche ein System im Auftrag einer Organisation prüfen und dabei die entdeckten Schwachstellen nicht selber ausnutzen sondern gegen eine Belohnung (Bounty) dokumentieren, melden und bei deren Schliessung unterstützen (NCSC, 2022b, S. 4). Im Gegenzug zu den Penetrationstests geschieht dies aber meist über eine öffentliche Plattform zur Nutzung des Schwarmwissens, einer breiteren Definition des Untersuchungsgegenstandes und über einen längeren Zeitraum, respektive ohne zeitliche Begrenzung. Da speziell die modernen Ransomware-Angriffe grossflächig und automatisiert ablaufen (BSI, 2021, S. 2), ist eine dauernde Anwendung der Sicherheitsmassnahmen zielführender als einzelne Testphasen.

Dabei sind BBP an sich nichts neues; so offerierte die Firma Netscape bereits im Jahre 1995 eine Belohnung, wenn eine Schwachstelle in ihrer Software gemeldet wurde (Kuehn & Mueller, 2014, S. 4). Jedoch haben die Anzahl BBP insbesondere seit 2013 stark zugenommen (Walshe & Simpson, 2020, S. 36).

### 2.4.2 Kosten

Die Belohnung für eine aufgedeckte Sicherheitslücke variiert je nach deren Schweregrad. Eine Analyse der Bug-Bounty-Plattform «HackerOne» von Walshe und Simpson (2020, S. 38) zeigt, dass der Bonus für eine aufgedeckte Sicherheitslücke mit tiefem Schweregrad im Durchschnitt bei USD 225.00 und bei einer kritischen Sicherheitslücke USD 7'924.00 beträgt. Dazu kommen die Kosten für den Betrieb, respektive die Nutzung, der Plattform. Für den Betrieb eines Vollzeitprogrammes ermittelten Walshe und Simpson (2020, S. 40) jährliche Kosten von USD 83'815.00 was ca. 128 Stellenprozent in der Informatik entspricht (auf Basis einer in London angestellten IT-Fachperson per Juli 2019). Die Schweizerische Post hat bei ihrem ersten privaten Bug-Bounty-Programm für 130 Schwachstellen Belohnungen über CHF 150'000.00 ausbezahlt, wodurch eine Schwachstelle im Durchschnitt eine Bounty von rund CHF 1'554.00 auslöste (Nafzger, 2021). Das andauernde, nun via Plattform «Yes we hack» öffentlich durchgeführte Bug-Bounty-Programm zur Identifikation von Sicherheitslücken im E-Voting-System der Schweizerischen Post bietet Belohnungen von CHF 1'000.00 bis CHF 230'000.00 (YesWeHack, 2023).

### 2.4.3 Einsatzbereich

Speziell die IT-affinen Internet- und Softwarefirmen wie Google, Mozilla und Samsung begannen mit der experimentellen Nutzung von BBP (Kuehn & Mueller, 2014, S. 4f.). In Bezug auf die öffentliche Verwaltung startete im April 2016 die USA unter dem Titel «Hack the Pentagon» erfolgreich mit ihrem ersten BBP (US Department of Defence, 2016). Unter EU-FOSSA 2 lancierte die Europäische Kommission im Januar 2019 ein BBP, welches 130 validierte Schwachstellen zutage förderte (Generaldirektion Informatik der Europäischen Kommission, 2019). Zuletzt lancierte 2021 die Schweizer Bundesverwaltung ein erfolg-

reiches BBP-Pilotprojekt, welches nun ausgeweitet und dauerhaft etabliert werden soll (NCSC, 2021, S. 3). Über die Nutzung von BBP in Gemeinden ist aktuell wenig bekannt.

## 2.5 Akzeptanz von Technologien

Der Bereich Bug Bounty ist noch wenig erforscht, insbesondere im öffentlichen Sektor. Einer Recherche in den umfassenden Wissenschaftsdatenbanken von Emerald Insight, Researchgate und Web of Science zufolge, fanden sich mit dem offenen Begriff «Bug Bounty» lediglich zwischen 19 und 100 Treffer. Nach einer zusätzlichen Einschränkung der Suche durch die Einbindung des booleschen Operator AND mit dem Wort «administration» fanden sich noch maximal acht Resultate. Bei deren Analyse musste festgestellt werden, dass sich bisher keine Arbeit auf die Akzeptanz von Bug Bounty Programmen fokussiert hat. Aus diesem Grund werden nachfolgend bestehende Theorien zur Akzeptanz von Technologien hinzugezogen.

### 2.5.1 DOI: Diffusion of Innovation Theory

Die von Rogers (1983) eingeführte Diffusion of Innovation Theory (DOI) ist eine weit verbreitete Grundlagentheorie für Studien betreffend die Akzeptanz und Verbreitung von IT-Innovationen (Mustonen-Ollila & Lyytinen, 2003, S. 1). Es wurde festgestellt, dass die Wahrnehmung einer Innovation durch die Entscheidungstragenden die Nutzungsabsicht eines neuen Produkts beeinflusst und dass die fünf Innovationsmerkmale relativer Vorteil, Kompatibilität, Komplexität, Testbarkeit sowie Beobachtbarkeit, die Wahrnehmung von Innovationen positiv wie auch negativ beeinflussen können (Rogers, 1983, S. 238ff.).

Die Literatur zeigt, dass DOI eine gut etablierte Theorie ist und die fünf Merkmale in Bezug auf die Ermittlung der Akzeptanz von IT-Innovationen in verschiedenen Studien erfolgreich eingesetzt wurden (Mustonen-Ollila & Lyytinen, 2003, S. 294; Min et al., 2019, S. 778). In der Literatur hat sich gezeigt, dass die wahrgenommenen relativen Vorteile wie Benutzerfreundlichkeit und wirtschaftliche Anreize einen positiven Einfluss auf Adaptionsentscheidungen haben (Mus-

tonen-Ollila & Lyytinen, 2003, S. 284). Die technische Kompatibilität und der relative Vorteil erhöhen die Akzeptanz von Lösungen für den elektronischen Datenaustausch deutlich (Premkumar et al., 1994, S. 183). Min et al. (2019, S. 778) bestätigen in ihrer Studie über die mobile App «Uber» den positiven Einfluss von relativem Vorteil, technischer Kompatibilität und Beobachtbarkeit auf den wahrgenommenen Nutzen, respektive die wahrgenommene Benutzerfreundlichkeit, und somit auf die Nutzungsabsicht. Bradford und Florin (2003, S. 220f.) fanden in ihrer Studie über die Einführung von ERP-Systemen hingegen keine signifikante Auswirkung der technischen Kompatibilität, was darauf hindeutet, dass die Konsistenz und Genauigkeit der DOI-Studien gewisse Schwächen aufweist (Karahanna et al., 1999, S. 184). Um diese Schwächen zu beheben, haben einige Forschende DOI mit anderen Theorien kombiniert, um einen repräsentativeren Rahmen zu schaffen, der die Interaktion zwischen Einstellung, Absicht und Verhalten berücksichtigt. Theorien zur Post-Adaption wie das Technologieakzeptanzmodell (TAM) und die Theorie des geplanten Verhaltens wurden eingesetzt, um die individuellen Wahrnehmungen vor und nach der Adaption zu untersuchen (Karahanna et al., 1999, S. 186).

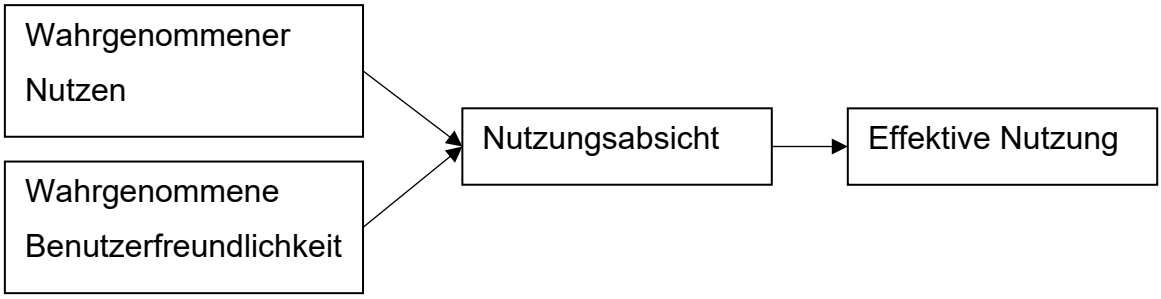
Auf dem Gebiet der Cybersicherheit wurde die DOI-Theorie ebenfalls angewandt. In einer Studie über die individuelle Absicht zur Nutzung von Anti-Spyware-Software fanden Lee und Kozar (2008, S. 115) heraus, dass relativer Vorteil, Kompatibilität, Beobachtbarkeit und Testbarkeit, wichtige Faktoren für die Einstellung einer Person gegenüber Anti-Spyware-Software waren, während die Benutzerfreundlichkeit hingegen keinen signifikanten Einfluss darstellte. In einer anderen Studie über die Akzeptanz von Sicherheitsmassnahmen für IT-Systeme durch die Arbeitnehmenden deuteten die Ergebnisse darauf hin, dass die wahrgenommene Nützlichkeit und die wahrgenommene Benutzerfreundlichkeit keinen grossen Einfluss auf die Absicht hatten, die Massnahmen umzusetzen (Jones et al., 2010, S. 14). Die Forschenden nehmen hierbei an, dass aufgrund der Verpflichtung Sicherheitsmassnahmen einzusetzen, die Benutzerfreundlichkeit nicht so stark ins Gewicht fällt; was zwar der Literatur widerspricht, aber mit den Ergebnissen der Studie über die Akzeptanz von Anti-

Spyware-Software übereinstimmt (Jones et al., 2010, S. 14). Darüber hinaus legen die Unternehmen im Zusammenhang mit der Informationssicherheit (IS) möglicherweise mehr Wert auf den Schutz als auf die Benutzerfreundlichkeit. Die Akzeptanz von innovativen Technologien könnte daher vom Nutzungskontext abhängig sein. Weitere Faktoren wie die Unterstützung durch das Management und die Organisation von Schulungen hatten einen positiven Einfluss auf die Akzeptanz, respektive die Nutzungsabsicht (Jones et al., 2010, S. 14). Obwohl DOI erfolgreich in Studien zu IT-Innovationen eingesetzt wurde, haben Hameed et al. (2012, S. 12) neben der Inkonsistenz eine weitere Einschränkung angeführt: Sie wird häufig zur Untersuchung des Verhaltens und der Einstellung von Einzelpersonen bei der Adaption von Innovationen angewendet und kann nicht den gesamten Prozess der Innovationsadaption erklären. Daher könnte die DOI-Theorie allein unzureichend sein, um die Übernahme von Innovationen in Organisationen vollständig zu erklären (Hameed et al., 2012, S. 12).

### 2.5.2 TAM: Technology Acceptance Model

Das Technology Acceptance Model (TAM) von Davis (1985) gilt als robustes, sparsames und einflussreiches Modell zur Erklärung des Akzeptanzverhaltens in Bezug auf Informatikmittel (Igbaria et al., 1995, S. 89; Mathieson, 1991, S. 20). Als Basis von TAM dient die von Ajzen und Fishbein (1980) entwickelte «theory of reasoned action», welche davon ausgeht, dass die Einstellung und subjektive Normen die Verhaltensabsicht beeinflusst, welche wiederum zu einer effektiven Verhaltensweise führt. TAM, siehe Visualisierung in Abbildung 6, geht davon aus, dass der wahrgenommene Nutzen und die Benutzerfreundlichkeit die Hauptdeterminanten für die Adaption von IT-Innovationen sind, indem die beiden Variablen die Nutzungsabsicht bestimmen und daraus das tatsächliche Nutzungsverhalten entsteht (Davis, 1985, S. 24).

**Abbildung 6: Technologieakzeptanzmodell**




*Anmerkung*: Eigene Darstellung nach Davies (1985, S. 24)

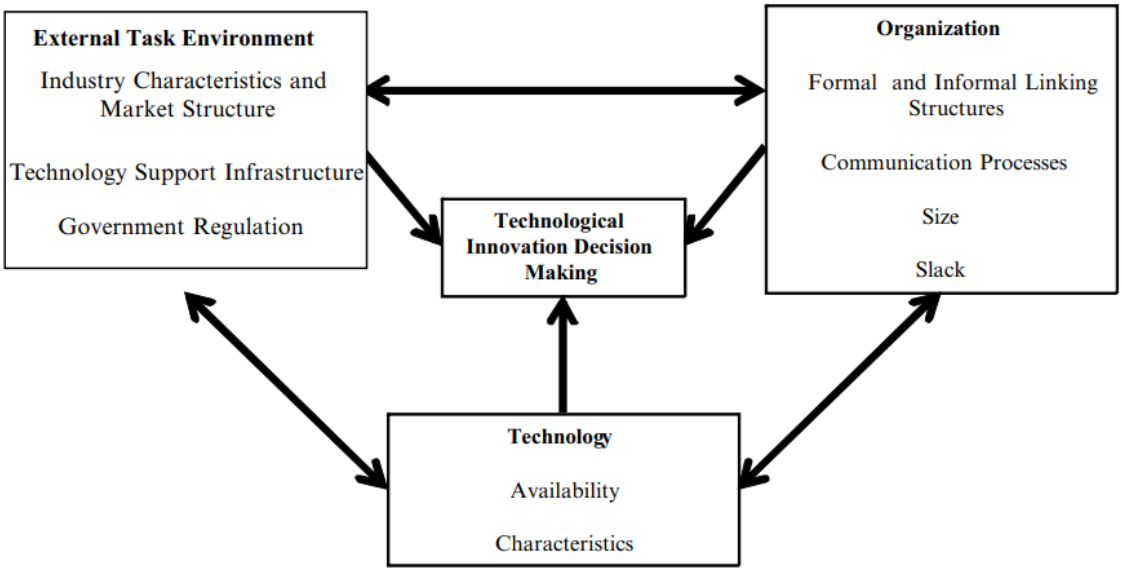
Im Laufe der Jahre hat TAM umfangreiche empirische Unterstützung durch Validierungen, Anwendungen und Replikation für seine Fähigkeit zur Vorhersage der Nutzung von Informationssystemen erhalten (Mathieson, 1991, S. 21; Horton et al., 2001, S. 246). Andererseits haben Forschende erkannt, dass die Allgemeingültigkeit von TAM keine aussagekräftigen Informationen über die Meinung der Nutzenden zu einem bestimmten System liefert. TAM muss zusätzliche Faktoren in andere IT-Akzeptanzmodelle integrieren, um seinen erklärenden Nutzen zu verbessern (Hu et al., 1999, S. 108). Das TAM-Modell ist mit seinen zwei erklärenden Variablen zu simpel, um eine Vielzahl von Anwendungsfällen abzudecken (Bagozzi, 2007, S. 244).

Inzwischen wurde das TAM-Modell in verschiedenen Situationen erweitert, um es anschaulicher und aussagekräftiger zu gestalten. Venkatesh und Davis präsentierten im Jahr 2000 das überarbeitete Modell TAM2. Dabei wurde das Modell um die unabhängige Variable subjektive Norm und die zwei Moderatoren Erfahrung und Freiwilligkeit ergänzt, wodurch der Erklärungsgehalt gesteigert werden konnte (Venkatesh & Davis, 2000, S. 198). Im Jahr 2008 folgte die letzte Erweiterung mit der Veröffentlichung von TAM 3, welches sich auf die Interventionsmöglichkeiten von Managern konzentriert (Venkatesh & Bala, 2008, S. 274f.).

### 2.5.3 TOE: Technology-Organization-Environment-Framework

Das Technologie-Organisation-Umwelt-Framework (TOE) wurde 1990 von Tornatzky und Fleischer entwickelt. Es definiert die drei Dimensionen Technologie, Organisation und Umwelt, welche den Diffusions- und Adaptionsprozess von Innovationen in Unternehmen beeinflussen (Tornatzky & Fleischer, 1990, S. 76). Das Modell wird in Abbildung 7 dargestellt. Das Literaturreview von Oliveira und Martins (2011, S. 113ff.) zeigt, dass TOE über eine solide theoretische Grundlage verfügt und in einer Vielzahl von Studien über die Adaption von IT-Innovationen in Organisationen angewendet wurde.

**Abbildung 7: TOE-Framework**




*Anmerkung:* Darstellung von Baker (2012, S. 236)

In einer Studie über die Einführung von Enterprise Resource Planning-Systemen in taiwanesischen Unternehmen wendeten Pan und Jang (2008, S. 95f.) das TOE-Framework an, um die Faktoren im jeweiligen Kontext zu ermitteln, welche sich auf die Einführung der Innovationen auswirken. Die Studie ergab, dass insbesondere Verbesserungen der Produktivität sowie die Unternehmensgrösse positiv mit der Einführung zusammenhängen, während wahrgenommene Hindernisse einen negativen Effekt haben (Pan & Jang, 2008, S. 100). Daher leiten die Autoren ab, dass die Unterstützung durch das Top-Management ein wichtiger Faktor für die Adaption von Innovationen ist.

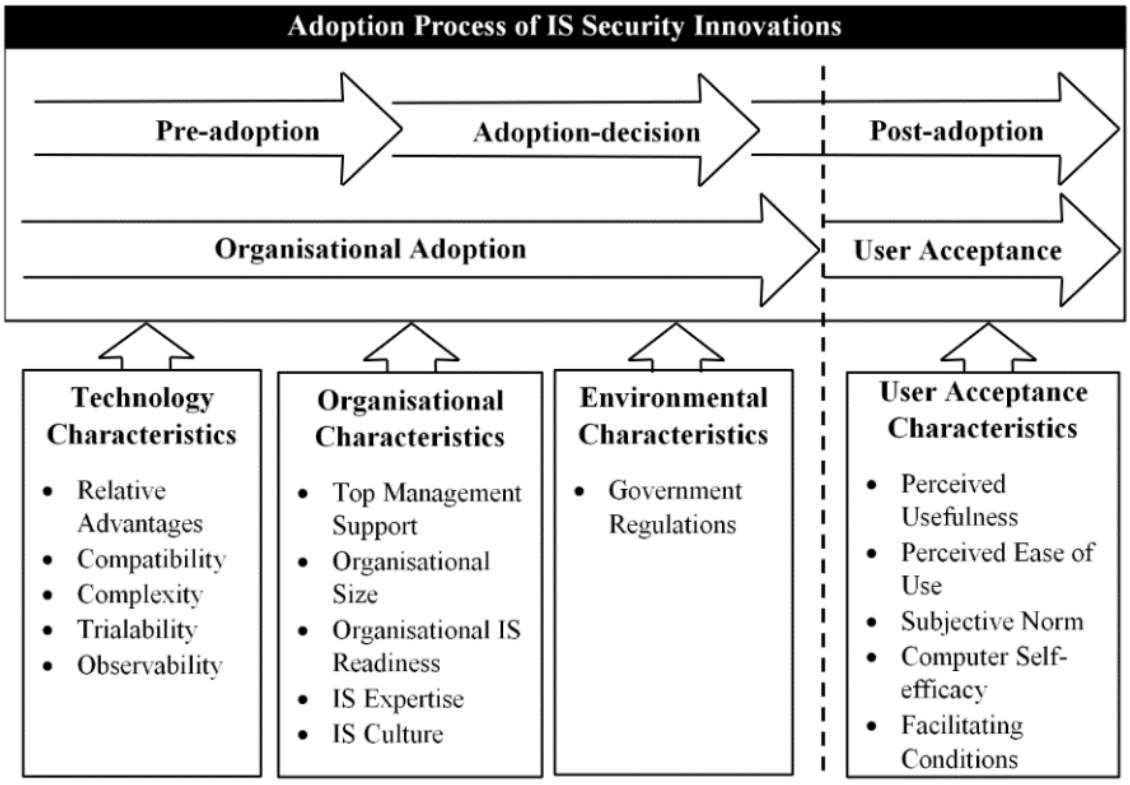
Nach Pan und Jang (2008, S. 99) konnte nur bei diesen drei Faktoren eine Signifikanz nachgewiesen werden, was im Widerspruch zu einer Reihe von anderen Studien über IT-Innovationen steht, die das Gegenteil gezeigt haben (Premkumar et al., 1994, S. 177; Wang et al., 2010, S. 812). Dies deutet darauf hin, dass der TOE-Rahmen Schwächen betreffend die Konsistenz aufweist. TOE hat hingegen durch die Einführung des Umweltkontexts Einschränkungen anderer Innovationstheorien erfolgreich überwunden, da dieser sowohl Chancen als auch Hindernisse für die Verbreitung und Übernahme von Innovationen bietet (Oliveira & Martins, 2011, S. 119).

### 2.5.4 Synthetisiertes Modell und deren Einflussfaktoren

Hameed und Arachchilage (2017) schlagen ein Modell (siehe Abbildung 8) zur Adaption von Innovationen im Bereich der Sicherheit von Informationssystemen in Organisationen vor, welches eine Kombination von DOI, TAM, Theory of planned behaviour (TPB) und TOE vorsieht. Durch diese Kombination von DOI, TAM und TPB kann ein Modell abgeleitet werden, welches die Adaption von IT-Sicherheitsinnovationen in drei Phasen (vor Einführung der Innovation, Einführungsentscheid, nach der Einführung der Innovation) widerspiegelt (Hameed & Arachchilage, 2017, S. 19). Sowohl TAM als auch TPB dienen zur Vorhersage und Erklärung der Akzeptanz durch Nutzende von Innovationen in empirischen Studien (Hameed & Counsell, 2014, S. 1). Gleichzeitig wird durch die Ergänzung von TPB mittels TAM dessen Erklärungs- und Vorhersagekraft erhöht (Awa et al., 2015, S. 88). Damit das von Hameed und Arachchilage (2017) synthetisierte Modell auf der Organisationsebene berücksichtigt werden kann, muss die integrative Darstellung der eingesetzten Modelle in einem kontextuellen Rahmen kombiniert werden. Hierfür wird das TOE-Framework hinzugezogen, welches bereits umfassend für die Untersuchung der Einführung von IT-Innovationen in Organisationen eingesetzt wurde (vergleiche Kapitel 2.5.3).

Im Kontext der Adaption von Innovationen in der IT-Sicherheit konnte ein angepasstes TOE-Framework («Sec-TOE») ebenfalls verifiziert werden (Salleh & Janczewski, 2016, S. 3). Ein integratives Modell aus DOI, TAM, TPB und TOE würde somit vollständig die Einführung von IT-Sicherheitsinnovationen in Organisationen erklären (Hameed & Arachchilage, 2017, S. 18).

**Abbildung 8: Vorgeschlagenes Modell zur Einführung von Informationssicherheitsinnovationen in Organisationen**




*Anmerkung*: Darstellung von Hameed und Arachchilage (2017, S. 19)

# 3 Modell und Hypothese

Basierend auf den theoretischen Grundlagen im vorangehenden Kapitel 2 werden die Forschungsfrage und das Konzeptmodell deduktiv abgeleitet und nachfolgend erläutert.

## 3.1 Forschungsfrage

Das Modell von Hameed und Arachchilage (vergleiche Abbildung 8) kombiniert verschiedene Theorien, um die Adaptionen von Innovationen in Organisationen zu beschreiben. Jedoch wurde das Modell bisher nicht im Feld getestet. Daher soll im Rahmen der vorliegenden Arbeit folgende Frage beantwortet werden:

> *Welche Voraussetzungen müssten erfüllt sein, um ein Bug-Bounty-Programm auf Ebene Gemeinde zu etablieren?*

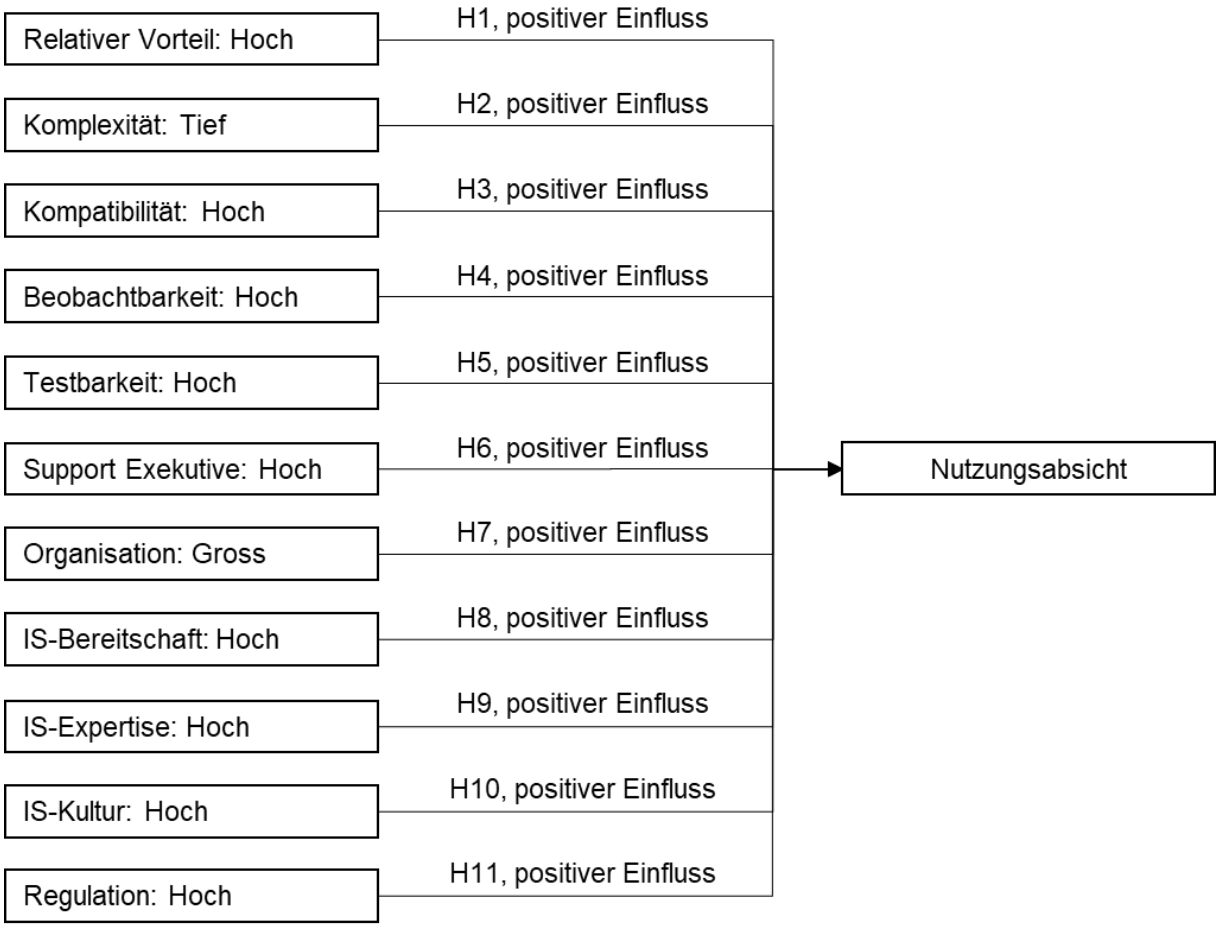
Zur Beantwortung der leitenden Forschungsfrage werden nachfolgende untergeordnete Fragestellungen definiert:

- Welche technologischen Voraussetzungen sind für die Einführung von Bug-Bounty-Programmen auf Ebene Gemeinde notwendig?
- Welche organisatorischen Voraussetzungen sind für die Einführung von Bug-Bounty-Programmen auf Ebene Gemeinde notwendig?
- Welche Voraussetzungen der Umwelt sind für die Einführung von Bug-Bounty-Programmen auf Ebene Gemeinde notwendig?

## 3.2 Konzeptmodell und Hypothesen

Das theoretisch abgeleitete Konzeptmodell in Abbildung 9 basiert im Grundsatz auf dem Modell von Hameed und Arachchilage in Abbildung 8. Da der Fokus jedoch auf die Adaption von Innovationen auf Ebene der Organisation liegt, wurden die Faktoren betreffend die User-Akzeptanz ausgelassen. Im Konzeptmodell bildet die Nutzungsabsicht die abhängige Variable, welche durch die unabhängigen Variablen relativer Vorteil, Komplexität, Kompatibilität, Beobachtbarkeit, Testbarkeit, Support der Exekutive, Organisationsgrösse, IS-Bereitschaft, IS-Expertise, IS-Kultur und Regulation beeinflusst wird.

**Abbildung 9: Konzeptmodell**




*Anmerkung:* Eigene Darstellung.

Dementsprechend werden die zu testenden Hypothesen in Bezug auf die Nutzung von innovativen Massnahmen zur Erhöhung der Informationssicherheit, wie zum Beispiel Bug-Bounty-Programme, wie folgt formuliert.

**H1** Die Nutzungsabsicht ist höher, wenn der relative Vorteil hoch ist (Hameed & Arachchilage, 2017, S. 20; Lee & Kozar, 2008, S. 115; Premkumar et al., 1994, S. 183)

**H2** Die Nutzungsabsicht ist höher, wenn die Komplexität tief ist (Hameed & Arachchilage, 2017, S. 21; Rogers, 1983, S. 239).

**H3** Die Nutzungsabsicht ist höher, wenn die Kompatibilität hoch ist (Hameed & Arachchilage, 2017, S. 21; Lee & Kozar, 2008, S. 115; Premkumar et al., 1994, S. 183).

**H4** Die Nutzungsabsicht ist höher, wenn die Beobachtbarkeit hoch ist (Hameed & Arachchilage, 2017, S. 22; Lee & Kozar, 2008, S. 115; Min et al., 2019, S. 778).

**H5** Die Nutzungsabsicht ist höher, wenn die Testbarkeit hoch ist (Hameed & Arachchilage, 2017, S. 21; Lee & Kozar, 2008, S. 115).

**H6** Die Nutzungsabsicht ist höher, wenn die Unterstützung durch die Exekutive hoch ist (Hameed & Arachchilage, 2017, S. 23; Pan & Jang, 2008, S. 100).

**H7** Die Nutzungsabsicht ist höher, wenn die Organisation grösser ist (Hameed & Arachchilage, 2017, S. 24; Pan & Jang, 2008, S. 100; Salleh & Janczewski, 2016, S. 3).

**H8** Die Nutzungsabsicht ist höher, wenn die IS-Bereitschaft höher ist (Hameed & Arachchilage, 2017, S. 24; Salleh & Janczewski, 2016, S. 12).

**H9** Die Nutzungsabsicht ist höher, wenn die IS-Expertise höher ist (Hameed & Arachchilage, 2017, S. 24; Safa et al., 2015, S. 75; Salleh & Janczewski, 2016, S. 12).

**H10** Die Nutzungsabsicht ist höher, wenn die IS-Kultur höher ist (Hameed & Arachchilage, 2017, S. 25; Safa et al., 2015, S. 75; Salleh & Janczewski, 2016, S. 12).

**H11** Die Nutzungsabsicht ist höher, wenn die Regulation hoch ist (Hameed & Arachchilage, 2017, S. 25; Looi, 2005, S. 71).

# 4 Forschungsdesign

In diesem Kapitel werden das methodische Vorgehen sowie die Stichprobe und die Gestaltung des Fragebogens erläutert.

## 4.1 Methodisches Vorgehen

Es wurde eine quantitative Studie in Form einer Onlineumfrage bei den Gemeindeverwaltungen, respektive den IT-Verantwortlichen der Gemeinde, durchgeführt. Die Literaturrecherche hat keine Ergebnisse auf die Frage geliefert, wie die Akzeptanz von Bug-Bounty-Programmen in der öffentlichen Verwaltung beeinflusst wird. Daher soll das bestehende theoretische Framework zur Adaption von Innovationen im Bereich der Sicherheit von Informationssystemen in Organisationen von Hameed und Arachchilage (2017) überprüft werden. Hierzu eignet sich die quantitative empirische Forschung (Röbken & Wetzel, 2016, S. 12). Die Anwendung eines Fragebogens zur Gewinnung von Erkenntnissen im Zusammenhang mit der Adaption von Massnahmen zu Steigerung der IT-Sicherheit wurde zudem bereits erfolgreich bei thematisch ähnlichen Studien angewendet (Lee & Kozar, 2008, S. 112f.; Salleh & Janczewski, 2016, S. 7).

Die Befragung wurde im Zeitraum vom 31. März 2023 bis 28. April 2023 durchgeführt. Da kein Stimulus manipuliert und keine Randomisierung der unabhängigen Variable vorgenommen wurde, handelt es sich bei der vorliegenden Umfrage um das verbreitete Ex-post-facto-Design (Stein, 2019, S. 131). Die Teilnehmenden werden dabei nach Abschluss der Umfrage (Ex-post) in zwei Gruppen mit einer positiven Nutzungsabsicht sowie einer negativen Nutzungsabsicht von Bug-Bounty-Programmen eingeteilt und untersucht. Dadurch sind rein korrelativen Aussagen möglich (Stein, 2019, S. 131).

## 4.2 Stichprobe

Die Grundgesamtheit umfasst alle Gemeinden der Deutschschweiz. Der Versand umfasste alle 1’382 Gemeinden (vergleiche Kapitel 1.4), welche somit zur Beantwortung der Umfrage eingeladen wurden (Selbstselektion der Teilnehmenden). Zur Anwendung des geplanten t-Tests werden zwei Gruppengrössen mit je mindestens 30 Teilnehmenden vorausgesetzt (Rasch et al., 2008, S. 59). Insgesamt haben 252 Gemeinden (Rücklaufquote 18.20 %) mit der Umfrage begonnen, wovon 171 die Umfrage vollständig abgeschlossen haben. Die Beendigungsquote der Umfrage beträgt somit 12.40 %.

## 4.3 Datenerhebung und Fragebogen

Zur Erhebung der Daten wurde aufbauend auf dem Framework von Hameed und Arachchilage (2017) ein Fragebogen entwickelt.

### 4.3.1 Aufbau

Der Fragebogen in Anhang 9.1 wurde anhand des Basismodelles von Hameed und Arachchilage (2017) gruppiert. Zu Beginn wurde die Bekanntheit von BBP erfragt. Personen, welche die Einstiegsfragen positiv beantwortet haben, wurden anschliessend gebeten, eine Definition von BBP vorzunehmen, um die Antworten zu verifizieren. Zudem wurde abgefragt ob bereits ein BBP durchgeführt wurde. Allen Teilnehmenden wurde danach eine standardisierte Definition von BBP präsentiert, um einen gleichen Wissenstand zu schaffen. Im Anschluss folgte die Erhebung der zu messenden Items betreffend die abhängigen und unabhängigen Variablen, sowie die demografischen Daten. Die Operationalisierung wird im nachfolgenden Kapitel erläutert.

### 4.3.2 Operationalisierung

Die Messung von abhängigen Variablen erfolgt in der wissenschaftlichen Literatur mehrheitlich durch Multi-Item-Skalen (Bruner, 2009, S. 240ff.). Dies wurde in der vorliegenden Arbeit jedoch als wenig praktikabel beurteilt, da die Teilnehmenden ein konkretes Konstrukt beurteilen sollten und der Fragebogen nicht zu lang sein sollte, um eine zu hohe Abbruchrate zu verhindern (Fuchs & Diaman-

topoulos, 2009, S. 196). Die Operationalisierung der abhängigen Variable Nutzungsabsicht erfolgte mit einer adaptierten Entscheidungsfrage auf Basis von Lee und Kozar (2008, S. 117): *Können Sie sich vorstellen, dass Ihre Gemeinde in Zukunft an einem Bug-Bounty-Programm teilnehmen wird?* Die weitere Operationalisierung der unabhängigen Variablen ist in Anhang 9.2 beschrieben. Die Messung erfolgte jeweils mit einer siebenstufigen Likert-Skala.

### 4.3.3 Pretest

Der Fragebogen wurde in einem zweistufigen Pretest geprüft. Nach den Empfehlungen von Neumann (2013, S. 99) wurde der Entwurf des Fragebogens zuerst durch zwei Personen beurteilt, bevor eine zweite Expertengruppe eine weitere Evaluation durchführte. In der ersten Phase hat die wissenschaftliche Betreuerin der vorliegenden Masterarbeit sowie eine Privatperson aus dem Umfeld des Autors den Fragebogen geprüft. Nach entsprechenden Anpassungen wurden drei weitere Personen für eine Validierung angefragt. Diese stammten aus der Zielgruppe der Umfrage. Nach deren Rückmeldung erfolgten finale Anpassungen und der Versand des Fragebogens via E-Mail.

## 4.4 Datenauswertung

Die Auswertung der Rohdaten erfolgte mittels der Statistiksoftware DATAtab. Die teilnehmenden Gemeinden wurden anhand der Differenzierungsfrage der Nutzungsabsicht in zwei Gruppen eingeteilt: Eine Gruppe mit positiver Nutzungsabsicht und eine Gruppe mit negativer Nutzungsabsicht von Bug-Bounty-Programmen. Deren Mittelwerte der unabhängigen Variablen wurden anschliessend miteinander verglichen, um Abweichungen zwischen den Gruppen zu evaluieren. Hierbei sollte grundsätzlich ein ungepaarter t-Test angewendet werden. Infolge fehlender Normalverteilung nach dem Shapiro-Wilk-Test wurde auf den Mann-Whitney-U-Test zurückgegriffen (Rasch et al., 2008, S. 59). Das Signifikanzniveau wurde auf 0.05 festgelegt.

## 4.5 Gütekriterien

In diesem Kapitel werden die Einhaltung der Gütekriterien Objektivität, Reliabilität und Validität beschrieben, damit die wissenschaftliche Qualität der Resultate gewährleistet werden kann.

Durch den Einsatz eines standardisierten Fragebogens wurde die Durchführungsobjektivität gewährleistet (Krebs & Menold, 2019, S. 491). Die Resultate der Umfrage werden offen und neutral dargelegt, um die Interpretation nachvollziehbar zu gestalten und hierdurch eine Auswertungsobjektivität zu schaffen (Krebs & Menold, 2019, S. 491).

Die Reliabilität setzt zuverlässige und stabile Ergebnisse voraus (Balzert et al., 2022, S. 27). Der standardisierte Fragebogen gewährleistet die Replizierbarkeit und Vergleichbarkeit der Ergebnisse. Die verständliche und objektive Formulierung wurde hierzu mittels eines zweistufigen Pretests geprüft. Im Rahmen der Auswertung werden zudem ausschliesslich anerkannte statistische Methoden angewendet, um eine Stabilität der Ergebnisse hervorzurufen.

Durch das Ex-post-facto-Design der Forschung können Störfaktoren nur schwierig kontrolliert werden (Stein, 2019, S. 132). Hierdurch wird die interne Validität gefährdet (Krebs & Menold, 2019, S. 501). Um die externe Validität zu gewährleisten, wird eine Übereinstimmung der Stichprobe mit der Population vorausgesetzt (Krebs & Menold, 2019, S. 500). Dies wird in den Resultaten unter Kapitel 5.1 entsprechend überprüft.

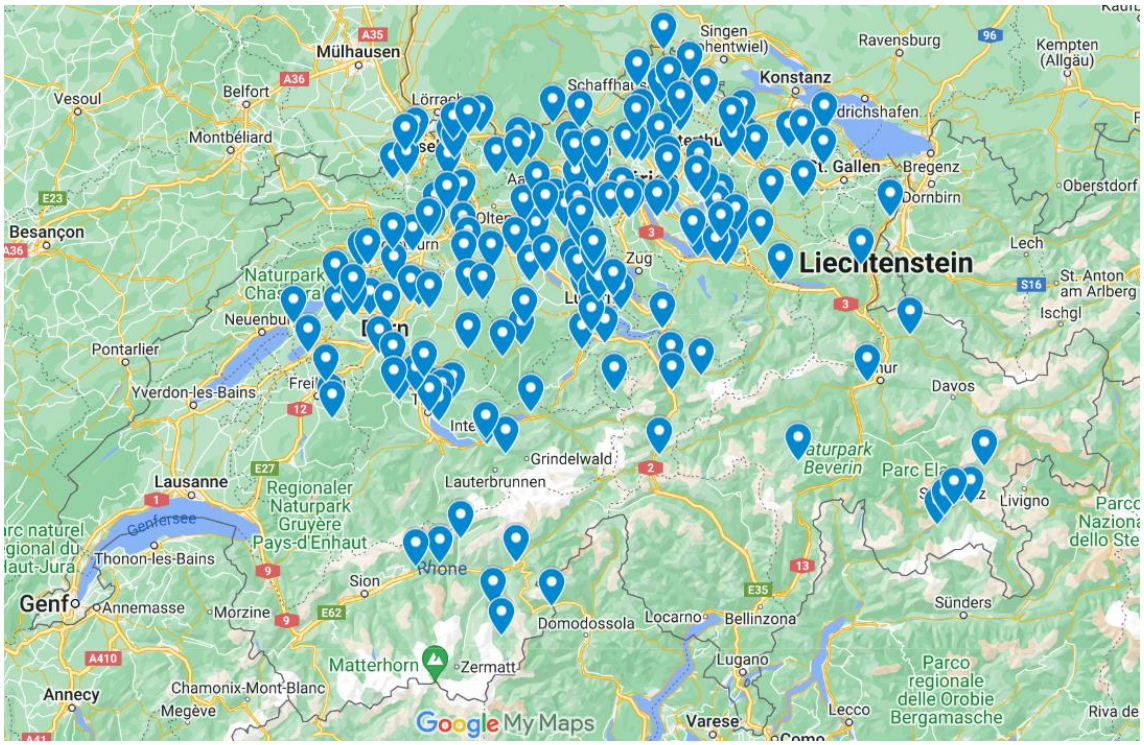
# 5 Resultate

Nachfolgend werden die Ergebnisse der Umfrage ausgewertet und präsentiert. Der Fokus liegt dabei auf der Nutzungsabsicht, und deren Einflussfaktoren aus den Bereichen Organisation, Technologie und Umwelt.

## 5.1 Beschreibung der Stichprobe

Wie die Abbildung 10 zeigt, stammen die Rückmeldungen aus der ganzen Schweiz. Einzig aus dem Sarganserland, sowie den Kantonen Schwyz, Glarus und den beiden Appenzell sind wenige bis keine Antworten eingetroffen. Aufgrund individueller Rückmeldungen der Gemeinden per Mail lässt sich dies dadurch begründen, dass in diesen Gebieten die Gemeindeinformatik zumeist im Verbund oder durch den Kanton betrieben wird. Daher fühlen sich die genannten Gemeinden nicht für die Informationssicherheit sachlich zuständig und haben auf eine Beantwortung der Fragen verzichtet.

**Abbildung 10: Karte der teilnehmenden Gemeinden**




*Anmerkung:* Eigene Darstellung mittels Google My Maps.

Tabelle 4 beschreibt die Attribute der Stichprobe in Bezug auf Grösse und Typologie der Gemeinden sowie Funktion der Teilnehmenden. Daraus wird ersichtlich, dass insbesondere ländliche Gemeinden und Gemeinden in der Grösse von 5'000 bis 19'999 Einwohnende in der Stichprobe übervertreten sind.

**Tabelle 4: Beschreibung der Stichprobe**

| **Grösse** | **Anzahl Stichprobe** | **Anteil Stichprobe** | **Anteil Population** |
|---|---|---|---|
| weniger als 1 000 Einwohner/innen | 28 | 16.37 % | 26.92 % |
| 1 000 - 1 999 Einwohner/innen | 27 | 15.79 % | 23.37 % |
| 2 000 - 4 999 Einwohner/innen | 48 | 28.07 % | 27.13 % |
| 5 000 - 9 999 Einwohner/innen | 38 | 22.22 % | 13.97 % |
| 10 000 - 19 999 Einwohner/innen | 24 | 14.04 % | 6.08 % |
| 20 000 - 49 999 Einwohner/innen | 5 | 2.92 % | 1.74 % |
| 50 000 - 99 999 Einwohner/innen | 1 | 0.58 % | 0.14 % |
| 100 000 und mehr Einwohner/innen | 0 | 0.00 % | 0.65 % |
| **Typologie** | **Anzahl Stichprobe** | **Anteil Stichprobe** | **Anteil Population** |
| Ländliche Gemeinde | 110 | 64.33 % | 49.06 % |
| Agglomerationsgemeinde | 43 | 25.15 % | 27.71 % |
| Urbane Gemeinde | 18 | 10.53 % | 23.23 % |
| **Outsourcing** | **Anzahl Stichprobe** | **Anteil Stichprobe** | |
| IT vollständig ausgelagert | 82 | 47.95 % | |
| IT teilweise ausgelagert | 61 | 35.67 % | |
| IT vollständig intern | 28 | 16.37 % | |
| **Funktion** | **Anzahl Stichprobe** | **Anteil Stichprobe** | |
| Gemeindeschreiber:in | 65 | 38.01 % | |
| Finanzverwalter:in | 26 | 15.20 % | |
| Leiter:in Informatik | 44 | 25.73 % | |
| Mitglied der Exekutive | 7 | 4.09 % | |
| Andere | 29 | 16.96 % | |

*Anmerkung:* Eigene Berechnung auf Basis der durchgeführten Umfrage, der ständigen Wohnbevölkerung per 31.12.2021 (BFS, 2022a) und der Raumgliederungen (BFS, 2023).

### Gruppenzusammensetzung

Die Zusammensetzung der beiden Untersuchungsgruppen (positive und negative Nutzungsabsicht) ist in Tabelle 5 ersichtlich. Dabei sind diverse Abweichungen ersichtlich, welche bei der Interpretation der Resultate berücksichtigt werden müssen, da hierdurch Verzerrungen möglich sind.

**Tabelle 5: Zusammensetzung der Untersuchungsgruppen**

| **Grösse** | **Gesamte Stichprobe** | **Positive NA** | **Negative NA** |
|---|---|---|---|
| weniger als 1 000 Einwohner/innen | 16.37 % | 8.75 % | 23.08 % |
| 1 000 - 1 999 Einwohner/innen | 15.79 % | 10.00 % | 20.88 % |
| 2 000 - 4 999 Einwohner/innen | 28.07 % | 33.75 % | 23.08 % |
| 5 000 - 9 999 Einwohner/innen | 22.22 % | 25.00 % | 19.78 % |
| 10 000 - 19 999 Einwohner/innen | 14.04 % | 18.75 % | 9.89 % |
| 20 000 - 49 999 Einwohner/innen | 2.92 % | 3.75 % | 2.20 % |
| 50 000 - 99 999 Einwohner/innen | 0.58 % | 0.00 % | 1.10 % |
| 100 000 und mehr Einwohner/innen | 0.00 % | 0.00 % | 0.00 % |
| **Typologie** | **Gesamte Stichprobe** | **Positive NA** | **Negative NA** |
| Ländliche Gemeinde | 64.33 % | 60.00 % | 68.13 % |
| Agglomerationsgemeinde | 25.15 % | 26.25 % | 24.18 % |
| Urbane Gemeinde | 10.53 % | 13.75 % | 7.69 % |
| **Outsourcing** | **Gesamte Stichprobe** | **Positive NA** | **Negative NA** |
| IT vollständig ausgelagert | 47.95 % | 41.25 % | 53.85 % |
| IT teilweise ausgelagert | 35.67 % | 40.00 % | 31.87 % |
| IT vollständig intern | 16.37 % | 18.75 % | 14.29 % |
| **Funktion** | **Gesamte Stichprobe** | **Positive NA** | **Negative NA** |
| Gemeindeschreiber:in | 38.01 % | 35.00 % | 40.66 % |
| Finanzverwalter:in | 15.20 % | 17.50 % | 13.19 % |
| Leiter:in Informatik | 25.73 % | 26.25 % | 25.27 % |
| Mitglied der Exekutive | 4.09 % | 5.00 % | 3.30 % |
| Andere | 16.96 % | 16.25 % | 17.58 % |

*Anmerkung:* Eigene Darstellung.

## 5.2 Faktoren Organisation

Der Einflussfaktor Organisation teilt sich wiederum in die Faktoren Support der Exekutive, Organisationsgrösse, IS-Bereitschaft (Bewusstsein und Erfahrung), IS-Expertise und IS-Kultur (Akzeptanz und Bewusstsein). Deren Ergebnisse sind in Tabelle 6 zusammengefasst und werden nachfolgend umschrieben.

**Tabelle 6: Deskriptive Statistik der Faktoren Organisation**

| | Positive Nutzungsabsicht | | | Negative Nutzungsabsicht | | |
|---|---|---|---|---|---|---|
| | N | M | SD | N | M | SD |
| Support der Exekutive | 80 | 5.23 | 1.17 | 90 | 4.24 | 1.36 |
| Organisationsgrösse | 80 | 3.65 | 1.91 | 91 | 3.43 | 1.65 |
| IS-Expertise Bewusstsein | 80 | 4.66 | 1.17 | 90 | 4.18 | 1.23 |
| IS-Expertise Erfahrung | 80 | 4.44 | 1.15 | 91 | 3.99 | 1.28 |
| IS-Bereitschaft | 79 | 3.53 | 1.39 | 90 | 2.89 | 1.41 |
| IS-Kultur Akzeptanz | 80 | 5.44 | 1.04 | 91 | 5.2 | 0.93 |
| IS-Kultur Bewusstsein | 80 | 4.71 | 1.14 | 91 | 4.68 | 1.01 |

*Anmerkung:* Eigene Darstellung.

### 5.2.1 Support der Exekutive

Der Support der Exekutive wird der Nutzungsabsicht von Bug-Bounty-Programmen gegenübergestellt. Dabei zeigt sich, dass bei einer positiven Nutzungsabsicht der Mittelwert des Supports bei 5.23 liegt, während bei einer negativen Nutzungsabsicht der Mittelwert 4.24 beträgt. Der Wert 5.23 signalisiert eher eine Zustimmung, während der Wert 4.24 eine neutrale Aussage darstellt.

Da der Shapiro-Wilk Test signifikant war ($p < 0.001$) und somit keine Normalverteilung der Daten festgestellt wurde, wurde ein nichtparametrisches Testverfahren angewendet. Der Mann-Whitney U-Test zeigte, dass der Unterschied zwischen positiver und negativer Nutzungsabsicht in Bezug auf die Variable Support der Exekutive auf dem definierten Signifikanzniveau von 5 % statistisch signifikant war ($U = 2098.5$, $p = <0.001$, $r = 0.37$).

### 5.2.2 Organisationsgrösse

Die Organisationsgrösse wurden mittels Anzahl Mitarbeitenden der Verwaltung erhoben, welche in sechs Gruppen eingeteilt wurden (Wert 1 = 1 – 4 Mitarbeitende / Wert 6 = 100 und mehr Mitarbeitende). Die mittlere Organisationsgrösse beträgt bei einer negativen Nutzungsabsicht von BBP 3.43 (tendenziell 10 bis 19 Mitarbeitende) während bei einer positiven Nutzungsabsicht der Mittelwert der Organisationsgrösse 3.65 (tendenziell 20 bis 49 Mitarbeitende) beträgt. Bei einer positiven Nutzungsabsicht sind somit tendenziell grössere Gemeindeverwaltungen zu finden. Der Mann-Whitney U-Test zeigte, dass dieser Unterschied aber nicht signifikant war ($U = 3368.5$, $p = 0.402$, $r = 0.07$).

### 5.2.3 IS-Expertise

Die IS-Expertise wurde wiederum in zwei Elemente geteilt. Darunter fällt das Bewusstsein über potenzielle Bedrohungen und die Erfahrung in deren Erkennung und Bewältigung. Der Mittelwert des Bewusstseins ist bei der Gruppe mit einer positiven Nutzungsabsicht mit 4.66 höher als bei der Gruppe mit negativer Nutzungsabsicht (Mittelwert 4.18). Diese Abweichung ist nach dem Mann-Whitney U-Test statistisch signifikant ($U = 2856$, $p = 0.02$, $r = 0.18$). Ein ähnliches Bild zeigt sich beim zweiten Element der IS-Expertise. Die Erfahrung ist bei den Organisationen mit positiver Nutzungsabsicht mit einem Mittelwert von 4.44 höher als bei den Organisationen mit negativer Nutzungsabsicht (Mittelwert von 3.99). Diese Differenz ist ebenfalls statistisch signifikant (Mann-Whitney-U-Test; $U = 2927$, $p = 0.028$, $r = 0.17$). Somit weisen beide Elemente der IS-Expertise einen signifikanten Einfluss auf die Nutzungsabsicht auf.

### 5.2.4 IS-Bereitschaft

Bei der IS-Bereitschaft wurde abgefragt, inwiefern personelle Ressourcen für den Einsatz von innovativen Massnahmen zur Erhöhung der Informationssicherheit eingesetzt werden können. Diese personellen Ressourcen werden bei der Gruppe mit einer positiven Nutzungsabsicht höher bewertet (Mittelwert 3.53) als bei der Gruppe mit negativer Nutzungsabsicht (Mittelwert 2.89). Nach dem Mann-Whitney-U-Test ist dieser Unterschied statistisch signifikant ($U = 2589$, $p = 0.002$, $r = 0.24$).

### 5.2.5 IS-Kultur

Die IS-Kultur wurde mit zwei Fragestellungen erhoben. Diese umfassen sowohl die Akzeptanz von Massnahmen zur Steigerung der Informationssicherheit bei den Mitarbeitenden wie auch das Bewusstsein der Mitarbeitenden in Sachen Informationssicherheit.

Bei der Akzeptanz zeigt sich, dass die Mittelwerte bei den Gemeinden mit positiver Nutzungsabsicht (Mittelwert 5.44) und mit negativer Nutzungsabsicht (Mittelwert 5.20) ähnlich hoch und eher zustimmend sind. Der Unterschied ist nach dem Mann-Whitney-U-Test nicht signifikant (U = 3213, p = 0.187, r = 0.11). Dasselbe gilt für den zweiten Faktor des Bewusstseins. Der Mittelwert beträgt hier bei einer positiven Nutzungsabsicht 4.71, während er sich bei einer negativen Nutzungsabsicht auf 4.68 beläuft. Auch diese Abweichung ist statistisch nicht signifikant (Mann-Whitney-U-Test; U = 3588, p = 0.873, r = 0.01).

### 5.2.6 Zusammenfassung der Faktoren Organisation

Die Resultate zeigen verschiedene Gruppenunterschiede zwischen den Gemeinden mit positiver und mit negativer Nutzungsabsicht von Bug-Bounty-Programmen auf (vergleiche Tabelle 7). Dabei wurde festgestellt, dass insbesondere bei den Faktoren Support der Exekutive, IS-Expertise (Bewusstsein und Erfahrung) sowie IS-Bereitschaft, signifikante Unterschiede bestehen. Nach Cohen (1988, S. 25f.) handelt es sich hierbei um kleine Effekte.

**Tabelle 7: Teststatistik Mann-Whitney-U-Test, Faktoren Organisation**

| Faktor | U | Z | p | r |
|---|---|---|---|---|
| Support der Exekutive | 2098.5 | -4.82 | <0.001* | 0.37 |
| Organisationsgrösse | 3368.5 | -0.85 | 0.402 | 0.07 |
| IS-Expertise Bewusstsein | 2856 | -2.39 | 0.020* | 0.18 |
| IS-Expertise Erfahrung | 2927 | -2.28 | 0.028* | 0.17 |
| IS-Bereitschaft | 2589 | -3.13 | 0.002* | 0.24 |
| IS-Kultur Akzeptanz | 3213 | -1.39 | 0.187 | 0.11 |
| IS-Kultur Bewusstsein | 3588 | -0.17 | 0.873 | 0.01 |

*Anmerkung:* Eigene Darstellung.
** Statistische Signifikanz auf 5 %-Niveau.*

## 5.3 Faktoren Technologie

Zu den Technologiefaktoren werden relativer Vorteil betreffend Kosten und Resultat, Komplexität, Kompatibilität, Beobachtbarkeit und Testbarkeit gezählt. Hierfür wurde den Teilnehmenden sechs Aussagen präsentiert und deren Zustimmung erhoben. Die Resultate sind in Tabelle 8 aufgeführt und werden in den nachfolgenden Kapiteln umschrieben.

**Tabelle 8: Deskriptive Statistik der Faktoren Technologie**

| | Positive Nutzungsabsicht | | | Negative Nutzungsabsicht | | |
|---|---|---|---|---|---|---|
| | N | M | SD | N | M | SD |
| Relativer Vorteil Kosten | 78 | 5.56 | 1.10 | 90 | 4.87 | 1.28 |
| Relativer Vorteil Resultat | 79 | 5.46 | 1.11 | 91 | 4.63 | 1.32 |
| Komplexität | 76 | 5.66 | 0.99 | 89 | 5.10 | 1.31 |
| Kompatibilität | 78 | 5.36 | 1.08 | 88 | 4.80 | 1.30 |
| Beobachtbarkeit | 79 | 5.52 | 1.04 | 90 | 4.76 | 1.17 |
| Testbarkeit | 79 | 5.37 | 1.20 | 89 | 4.85 | 1.41 |

*Anmerkung:* Eigene Darstellung.

### 5.3.1 Relativer Vorteil

Der relative Vorteil wird in Bezug auf Kosten (günstiger als Alternative) und Resultat (besseres Ergebnis als Alternative) untersucht. In beiden Bereichen weist die Gruppe mit einer positiven Nutzungsabsicht im Mittel eine höhere Zustimmung auf.

Beim relativen Vorteil Kosten weist die Gruppe mit positiver Nutzungsabsicht einen Mittelwert von 5.56 auf. Im Gegenzug beträgt das Mittel bei Gemeinden mit negativer Nutzungsabsicht 4.87. Diese Differenz ist gemäss Mann-Whitney U-Test statistisch signifikant ($U = 2407.5$, $p = <0.001$, $r = 0.28$). Dasselbe gilt beim relativen Vorteil Resultat. Hier liegt der Mittelwert bei 5.46 (positive Nutzungsabsicht), respektive 4.63 (negative Nutzungsabsicht). Diese Differenz ist ebenfalls statistisch signifikant (Mann-Whitney-U-Test; $U = 2279$, $p = <0.001$, $r = 0.33$).

### 5.3.2 Komplexität

Der Faktor Komplexität beschreibt die Einfachheit der Nutzung der neuen Technologie. Die Umfrageergebnisse zeigen dabei einen Unterschied in den Mittelwerten zwischen den beiden Gruppen mit positiver Nutzungsabsicht (Mittelwert 5.66) resp. negativer Nutzungsabsicht (Mittelwert 5.10). Dieser Unterschied ist nach dem Mann-Whitney-U-Test signifikant (U = 2574.5, p = 0.008, r = 0.22).

### 5.3.3 Kompatibilität

Die Übereinstimmung der Massnahme mit den eigenen Wertevorstellungen (Kompatibilität) wird in der Gruppe mit positiver Nutzungsabsicht (Mittelwert 5.36) höher bewertet als in der Gruppe mit negativer Nutzungsabsicht (Mittelwert 4.80). Der Unterschied in der Zustimmung ist statistisch signifikant (Mann-Whitney-U-Test; U = 2614.5, p = 0.008, r = 0.21).

### 5.3.4 Beobachtbarkeit

Die Gruppe mit positiver Nutzungsabsicht weist beim Faktor Beobachtbarkeit der Resultate einen höheren Mittelwert (5.52) auf als Gemeinden mit negativer Nutzungsabsicht (Mittelwert 4.76). Nach dem Mann-Whitney-U-Test ist dieser Unterschied statistisch signifikant (U = 2255.5, p = <0.001, r = 0.33).

### 5.3.5 Testbarkeit

Beim Faktor Testbarkeit zeigt sich bei der Gruppe mit positiver Nutzungsabsicht ein höherer Mittelwert in der Zustimmung. Dieser beträgt hier 5.37, während bei der Gruppe mit negativer Nutzungsabsicht der Mittelwert bei 4.85 liegt. Die Differenz ist nach dem Mann-Whitney-U-Test statistisch signifikant (U = 2797.5, p = 0.023, r = 0.18).

### 5.3.6 Zusammenfassung der Faktoren Technologie

Bei sämtlichen untersuchten Faktoren der Gruppe Technologie weisen Gemeinden mit einer positiven Nutzungsabsicht von Bug-Bounty-Programmen im Mittel höhere Zustimmungswerte auf. Wie die zusammengefassten Teststatistiken in Tabelle 9 zeigen, sind diese Unterschiede jeweils statisch signifikant. Nach Cohen (1988, S. 25f.) handelt es sich hierbei um kleine Effekte.

**Tabelle 9: Teststatistik Mann-Whitney-U-Test, Faktoren Technologie**

| Faktor | U | Z | p | r |
|---|---|---|---|---|
| Relativer Vorteil Kosten | 2407.5 | -3.63 | <0.001* | 0.28 |
| Relativer Vorteil Resultat | 2279 | -4.25 | <0.001* | 0.33 |
| Komplexität | 2574.5 | -2.77 | 0.008* | 0.22 |
| Kompatibilität | 2614.5 | -2.75 | 0.008* | 0.21 |
| Beobachtbarkeit | 2255.5 | -4.25 | <0.001* | 0.33 |
| Testbarkeit | 2797.5 | -2.36 | 0.023* | 0.18 |

*Anmerkung:* Eigene Darstellung.
** Statistische Signifikanz auf 5 %-Niveau.*

## 5.4 Faktoren Umwelt

Der Umweltfaktor besteht einzig aus der Regulation durch höhere Staatsebenen. Diese wird in drei Elemente Information über Wichtigkeit, Information über Nützlichkeit sowie Unterstützung bei der Kostensenkung geteilt und untersucht. Die zusammengefassten Ergebnisse in Tabelle 10 werden nachfolgend näher betrachtet.

**Tabelle 10: Deskriptive Statistik der Faktoren Umwelt**

| | Positive Nutzungsabsicht | | | Negative Nutzungsabsicht | | |
|---|---|---|---|---|---|---|
| | N | M | SD | N | M | SD |
| Wichtigkeit | 80 | 4.51 | 1.36 | 89 | 4.46 | 1.28 |
| Nützlichkeit | 80 | 4.29 | 1.34 | 90 | 4.06 | 1.30 |
| Kostensenkung | 80 | 3.53 | 1.38 | 88 | 3.33 | 1.27 |

*Anmerkung:* Eigene Darstellung.

### 5.4.1 Regulation Wichtigkeit

Die Information über die Wichtigkeit des Einsatzes von innovativen Massnahmen zur Steigerung der Informationssicherheit wird durch beide untersuchten Gruppen ähnlich bewertet. Der Mittelwert liegt bei 4.51 (Gruppe mit positiver Nutzungsabsicht), respektive 4.46 (Gruppe mit negativer Nutzungsabsicht). Der Unterschied ist nach dem Mann-Whitney-U-Test statistisch nicht signifikant ($U = 3523.5$, $p = 0.91$, $r = 0.01$).

### 5.4.2 Regulation Nützlichkeit

Die Information über die Nützlichkeit durch höhere Staatsebenen wird durch die Gruppe mit positiver Nutzungsabsicht im Mittel mit 4.29 bewertet. Im Vergleich dazu erreicht die Gruppe mit negativer Nutzungsabsicht einen Mittelwert von 4.06. Dieser Unterschied weist keine statistische Signifikanz auf (Mann-Whitney-U-Test; U = 3276, p = 0.313, r = 0.08).

### 5.4.3 Regulation Kostensenkung

Betreffend die Unterstützung zur Kostensenkung mittels neuer Massnahmen durch höhere Staatsebenen weist die Gruppe mit positiver Nutzungsabsicht einen Mittelwert von 3.53 auf. Die Gruppe mit negativer Nutzungsabsicht hingegen einen Mittelwert von 3.33. Dieser Unterschied ist nach Mann-Whitney-U-Test nicht statistisch signifikant (U = 3217, p = 0.337, r = 0.08).

### 5.4.4 Zusammenfassung der Faktoren Umwelt

Bei den drei untersuchten Bestandteilen zur Regulation im Faktor Umwelt konnten keine statistisch signifikanten Unterschiede zwischen den Gruppen mit positiver und negativer Nutzungsabsicht evaluiert werden. Nach Cohen (1988, S. 25f.) handelt es sich hierbei um sehr kleine Effekte.

**Tabelle 11: Teststatistik Mann-Whitney-U-Test, Faktoren Umwelt**

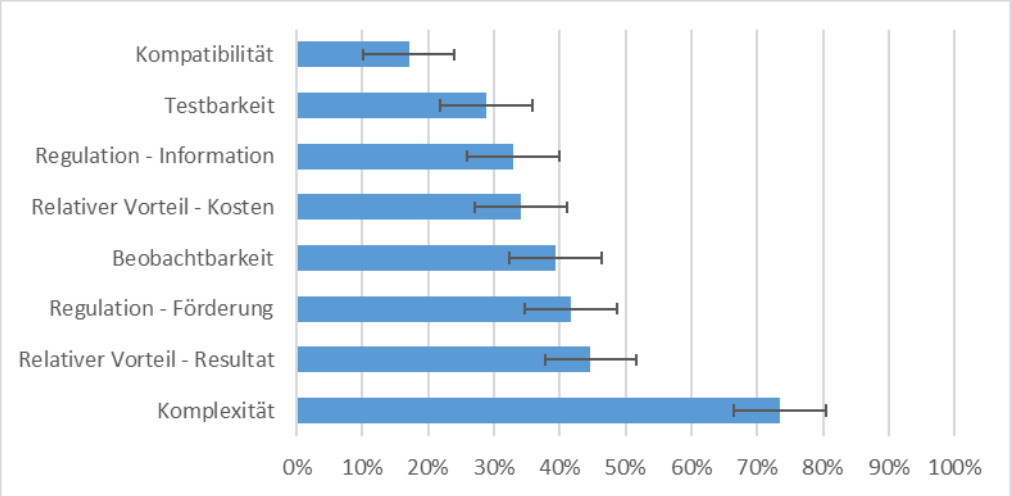
| Faktor | U | Z | p | r |
|---|---|---|---|---|
| Information Wichtigkeit | 3523.5 | -0.12 | 0.910 | 0.01 |
| Information Nützlichkeit | 3276 | -1.04 | 0.313 | 0.08 |
| Förderung Kostensenkung | 3217 | -0.99 | 0.337 | 0.08 |

*Anmerkung:* Eigene Darstellung.
** Statistische Signifikanz auf 5 %-Niveau.*

## 5.5 Relevanz der Faktoren

Die Teilnehmenden haben die Relevanz der vorgängig abgefragten Faktoren Technologie und Umwelt (siehe Kapitel 5.3 und 5.4) bewertet. Dabei wird aus Abbildung 11, respektive Tabelle 12, ersichtlich, dass der Faktor Komplexität für den Adaptionsentscheid am häufigsten genannt wurde. Unter Berücksichtigung der Fehlerspanne von 7-Prozenpunkten[1] ist der Faktor Komplexität gegenüber allen anderen Faktoren signifikant häufiger genannt worden. Der am zweithäufigsten genannte Faktor relativer Vorteil Resultat ist gegenüber den Faktoren Testbarkeit und Kompatibilität signifikant häufiger genannt worden, während sein Rang gegenüber den anderen untergeordneten Faktoren ein Zufallsergebnis sein könnte.

**Abbildung 11: Relevanz der Faktoren zur Adaption von innovativen IS-Massnahmen**




*Anmerkung:* Eigene Darstellung unter Berücksichtigung der Fehlerspanne, n = 170.

Unter Berücksichtigung der positiven und negativen Nutzungsabsicht in Bezug auf BBP lassen sich gemäss Tabelle 12 keine signifikanten Unterschiede feststellen. Alle Werte befinden sich innerhalb des Konfidenzintervalls auf einem Konfidenzniveau von 95 %.

[1] Stichprobe: 170 Gemeinden; Population: 1'382 Gemeinden; Konfidenzniveau: 95 %

**Tabelle 12: Relevanz der Faktoren zur Adaption von innovativen IS-Massnahmen**

| Faktor | Anteil | CI hoch | CI tief | Positive NA | Negative NA |
|---|---|---|---|---|---|
| Komplexität | 74% | 81% | 67% | 77% | 70% |
| Relativer Vorteil Resultat | 45% | 52% | 38% | 39% | 51% |
| Regulation Förderung | 42% | 49% | 35% | 40% | 44% |
| Beobachtbarkeit | 39% | 46% | 32% | 43% | 35% |
| Relativer Vorteil Kosten | 34% | 41% | 27% | 28% | 41% |
| Regulation Information | 33% | 40% | 26% | 31% | 35% |
| Testbarkeit | 29% | 36% | 22% | 31% | 26% |
| Kompatibilität | 17% | 24% | 10% | 17% | 18% |
| Andere | 2% | 9% | -5% | - | - |

*Anmerkung:* Konfidenzintervall (CI) bei Konfidenzniveau 95 %.

## 5.6 Erfüllung der Faktoren von Bug-Bounty-Programmen

Im vorangehenden Kapitel wurden die Resultate in Bezug auf die Relevanz der evaluierten Faktoren vorgestellt. Im Anschluss wurde abgefragt, inwiefern die Teilnehmenden denken, dass BBP diese Faktoren erfüllen. Mit Ausnahme des Faktors Testbarkeit beurteilen die Teilnehmenden mit einer positiven Nutzungsabsicht sämtliche Faktoren höher als die Teilnehmenden mit negativer Nutzungsabsicht.

**Tabelle 13: Deskriptive Statistik, Faktoren BBP**

| | Positive Nutzungsabsicht | | | Negative Nutzungsabsicht | | |
|---|---|---|---|---|---|---|
| **Faktor** | N | M | SD | N | M | SD |
| Relativer Vorteil Kosten | 64 | 4.11 | 1.35 | 47 | 3.81 | 1.50 |
| Relativer Vorteil Resultat | 66 | 4.86 | 1.18 | 51 | 4.10 | 1.69 |
| Komplexität | 63 | 4.32 | 1.29 | 47 | 3.66 | 1.45 |
| Kompatibilität | 64 | 4.38 | 1.42 | 49 | 3.71 | 1.32 |
| Beobachtbarkeit | 63 | 4.52 | 1.31 | 46 | 3.98 | 1.57 |
| Testbarkeit | 62 | 3.56 | 1.51 | 47 | 3.64 | 1.70 |
| Regulation Information | 64 | 2.83 | 1.28 | 51 | 2.39 | 1.25 |
| Regulation Förderung | 58 | 3.00 | 1.39 | 43 | 2.74 | 1.27 |

*Anmerkung:* Eigene Darstellung.

Die Abweichung in den Mittelwerten wurde mittels Mann-Whitney-U-Test auf deren statistische Signifikanz überprüft. Die dazugehörige Teststatistik ist in Tabelle 14 abgebildet. Die Abweichungen in den Mittelwerten ist bei den Faktoren relativer Vorteil Resultat (p = 0.015), Komplexität (p = 0.050) und Kompatibilität (p = 0.027) auf einem Signifikanzniveau von 95 % statistisch signifikant.

**Tabelle 14: Teststatistik Mann-Whitney-U-Test, Faktoren BBP**

| Faktor | U | Z | p | r |
|---|---|---|---|---|
| Relativer Vorteil Kosten | 1390 | -0.70 | 0.499 | 0.07 |
| Relativer Vorteil Resultat | 1238.5 | -2.51 | 0.015* | 0.23 |
| Komplexität | 1154.5 | -2.04 | 0.050* | 0.19 |
| Kompatibilität | 1185 | -2.30 | 0.027* | 0.22 |
| Beobachtbarkeit | 1153.5 | -1.87 | 0.071 | 0.18 |
| Testbarkeit | 1407.5 | -0.31 | 0.765 | 0.03 |
| Regulation Information | 1316 | -1.83 | 0.076 | 0.17 |
| Regulation Förderung | 1081 | -1.18 | 0.257 | 0.12 |

*Anmerkung:* Eigene Darstellung.
** Statistische Signifikanz auf 5 %-Niveau.*

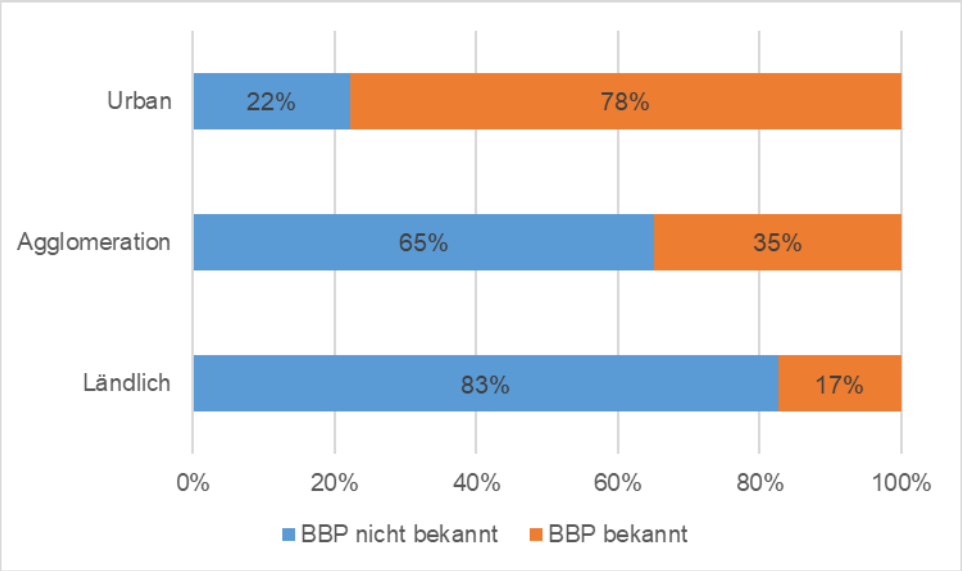
Bei der Auswertung ist auffällig, dass rund 2/3 der Teilnehmenden die Frage nicht beantwortet haben. Aus den optionalen Kommentaren wird ersichtlich, dass die fehlenden Erfahrungen mit, resp. das fehlende Vorwissen über BBP, keine qualifizierte Beurteilung der Teilnehmenden zulässt. Dies erklärt die hohe Anzahl an Antwortausfällen, was zu einer Schweigeverzerrung (Non-Respons Bias) führen kann.

## 5.7 Weitere Resultate

### 5.7.1 Bekanntheit und Nutzung

Unter den teilnehmenden Gemeinden sind BBP bei einer Mehrheit von 71.90 % unbekannt. Im Gegenzug wussten 28.10 % der Gemeinden, was ein BBP ist. Mittels einer Überprüfungsfrage konnte sichergestellt werden, dass die Personen, welche angaben ein BBP zu kennen, dieses auch erklären können. Wie die nachfolgende Abbildung 12 zeigt, sind BBP insbesondere bei Gemeinden aus dem urbanen Raum bekannt. Gemeinden aus der Agglomeration oder dem ländlichen Umfeld haben markant tiefere Bekanntheitswerte.

**Abbildung 12: Bekanntheit von BBP nach Gemeindetypologie**




*Anmerkung:* Eigene Darstellung, n = 171.

Von den 171 teilnehmenden Gemeinden kennen 48 die Funktionsweise von BBP. Von diesen 48 Gemeinden haben wiederum sechs Gemeinden (3.51 % aller Teilnehmenden) bereits ein BBP durchgeführt oder über eine Plattform teilgenommen. Die sechs Gemeinden, welche bereits praktische Erfahrungen mit BBP gesammelt haben, würden BBP auch in Zukunft einsetzen.

### 5.7.2 Verantwortungsbewusstsein

Neben den bereits untersuchten Faktoren wurde das Verantwortungsbewusstsein der Gemeinden abgefragt. Dabei wurde abgefragt, ob bei einem Datenverlust die Verantwortung extern (bei einem Dienstleister) oder intern (bei der Exekutive oder der zuständigen Abteilung) zu tragen ist. Die Resultate sind in Tabelle 15 aufgeführt. Zur Verifizierung der Abhängigkeit wurde ein $Chi^2$ Test zwischen der Variable Nutzungsabsicht und der Variable Verantwortung durchgeführt. Zwischen den beiden Variablen konnte ein statistisch signifikanter Zusammenhang festgestellt werden ($\chi^2(1) = 18.54$, $p = <0.001$, Cramér's $V = 0.33$).

Teilnehmende mit einer positiven Nutzungsabsicht von BBP sehen die Verantwortung für Datenverluste mehrheitlich intern (78 %), also bei der zuständigen Abteilung oder der Exekutive. Im Gegenzug sehen die Teilnehmenden mit einer negativen Nutzungsabsicht die Verantwortung tendenziell beim externen Dienstleister (54 %).

**Tabelle 15: Ergebnisse Faktor Verantwortung**

| | Externe Verantwortung | Interne Verantwortung | Total |
|---|---|---|---|
| Positive Nutzungsabsicht | 17 | 62 | 79 |
| Negative Nutzungsabsicht | 48 | 41 | 89 |
| Total | 65 | 103 | 168 |

*Anmerkung:* Darstellung in absoluten Werten.

# 6 Diskussion und Würdigung

In diesem Kapitel werden die vorstehenden Resultate aus der Datenerhebung unter Einbezug der theoretischen Grundlagen gewürdigt.

## 6.1 Faktoren Organisation

Auf Basis des Modells zur Adaption von IS-Massnahmen von Hameed und Arachchilage (2017, S. 19) wurde bei den Organisationsfaktoren insbesondere die Elemente Support der Exekutive (Top Management Support), Organisationsgrösse, IS-Expertise, IS-Bereitschaft und IS-Kultur untersucht. Dabei konnte bei den Elementen Support der Exekutive, IS-Expertise und IS-Bereitschaft eine signifikante Abweichung zwischen den Gruppen mit positiver oder negativer Nutzungsabsicht von BBP festgestellt werden. Gemeinden, welche eine positive Nutzungsabsicht gegenüber BBP haben, weisen dementsprechend eine höhere Unterstützung durch ihre Exekutive, höheres Bewusstsein über die Bedrohungslage, mehr Erfahrung im Umgang mit IS-Massnahmen und mehr personelle Ressourcen für den Einsatz von innovativen IS-Massnahmen auf.

Diese Ergebnisse reihen sich nur teilweise in die bestehende Forschung ein. So werden der Einfluss durch den Support der Exekutive von Pan und Jang (2008, S. 100) bestätigt, während Salleh und Janczewski (2016, S. 12) die Signifikanz von IS-Expertise und IS-Bereitschaft nachweisen konnten. Die beiden Forschungsteams haben in ihren jeweiligen Studien bei den Elementen Organisationsgrösse und IS-Kultur ebenfalls einen signifikanten Einfluss festgestellt, welcher in der vorliegenden Arbeit jedoch nicht bestätigt werden konnte. Dies lässt sich allenfalls auf den Umstand zurückführen, dass Massnahmen zur Steigerung der Informationssicherheit verpflichtend genutzt werden müssen, unabhängig von Grösse oder Arbeitskultur in der Gemeinde. Daher haben diese beiden Faktoren allenfalls einen untergeordneten Einfluss. Eine ähnliche Annahme wurde bereits durch Jones et al. (2010, S. 14) bei der Anwendung von DOI im Hinblick auf die Benutzerfreundlichkeit getroffen.

Aufgrund der vorliegenden Erkenntnisse werden die Hypothesen 7 (*Nutzungsabsicht ist höher, wenn die Organisation grösser ist*) und die Hypothesen 10 (*Nutzungsabsicht ist höher, wenn die IS-Kultur höher ist*) verworfen. Im Gegenzug werden die Hypothese 6 (*Nutzungsabsicht ist höher, wenn die Unterstützung durch die Exekutive höher ist*), die Hypothese 8 (*Nutzungsabsicht ist höher, wenn die IS-Bereitschaft höher ist*) und die Hypothese 9 (*Nutzungsabsicht ist höher, wenn die IS-Expertise höher ist*) angenommen.

## 6.2 Faktoren Technologie

Betreffend die Technologiefaktoren konnte bei allen Elementen eine signifikante Abweichung zwischen den untersuchten Gruppen festgestellt werden. Die Gruppe mit einer positiven Nutzungsabsicht weist in Bezug auf hohen relativen Vorteil, tiefe Komplexität, hohe Kompatibilität, hohe Beobachtbarkeit und hohe Testbarkeit durchwegs höhere Mittelwerte auf als die Gruppe mit negativer Nutzungsabsicht. Diese Faktorelemente wurden bereits in einer Vielzahl von ähnlichen Studien (z. B. Lee & Kozar, 2008, S. 115; Min et al., 2019, S. 778; Premkumar et al., 1994, S. 183) bestätigt und reihen sich daher gut in die bestehende Literatur ein.

Bei einer nachträglichen Betrachtung der Fragestellungen im Bereich der Technologiefaktoren muss festgehalten werden, dass deren Resultate fehleranfällig für die Interpretation sein könnten. Da die Fragen direkt auf die Nutzungsabsicht zielten (sinngemäss: «Wenn X erfüllt ist, nutzen wir Innovative IS-Massnahmen»), ist es wenig überraschend, dass diese bei den einzelnen Elementen höher ausfällt, wenn die generelle Nutzungsabsicht bereits vorhanden ist. Daher muss insbesondere die beurteilte Relevanz der Faktoren berücksichtigt werden. Dabei wird ersichtlich, dass der Faktor Komplexität die höchste Relevanz für den Adaptionsentscheid aufweist, unabhängig der Nutzungsabsicht von BBP. Die weiteren Elemente liegen jeweils innerhalb des Stichprobenfehlers, weshalb hier keine verlässlichen Aussagen über die weitere Rangfolge getätigt werden kann.

Die hohe Relevanz des Faktors Komplexität scheint grundsätzlich gut nachvollziehbar. Das Gemeindepersonal übernimmt speziell in kleineren Organisationen eine Vielzahl von verschiedenen Aufgaben. Die Digitalisierung und damit der Schutz der Informationssicherheit ergänzen den bereits sehr breiten Aufgabenkatalog um ein neues, hochkomplexes Themengebiet. Dass diese Zusatzaufgabe aus Sicht der Gemeindeverwaltung nicht zu viele Ressourcen infolge einer hohen Komplexität binden darf, erscheint daher als logische Schlussfolgerung. Wenn BBP in Gemeinden etabliert werden sollten, müssten diese somit eine einfache Nutzung garantieren.

Werden die untersuchten Elemente konkret in Bezug auf BBP betrachtet, zeigt sich, dass die Gruppe mit positiver Nutzungsabsicht den relativen Vorteil in Bezug auf die Ergebnisse, die Komplexität und die Kompatibilität signifikant höher beurteilen als die Gruppe mit negativer Nutzungsabsicht. Dies lässt darauf schliessen, dass insbesondere diese Elemente für den Adaptionsentscheid von BBP relevant sind. BBP können anscheinend mit diesen drei Faktoren überzeugen. Da bei diesen Fragestellungen ein grosser Anteil an Antwortausfällen zu verzeichnen sind, müssen diese Ergebnisse jedoch mit Zurückhaltung interpretiert werden. Die Ausfallrate lässt sich darin begründen, dass viele Gemeinden nicht genügend Wissen über BBP und sich daher kein Urteil erlauben wollen. Die beiden Untersuchungsgruppen weisen aber trotz der hohen Ausfallrate mehr als 30 Untersuchungsobjekte auf und können daher grundsätzlich als valide betrachtet werden.

Die Resultate der quantitativen Forschung zeigen, dass in der Gruppe Technologie alle Hypothesen von Nummer 1 bis zur Nummer 5 alle angenommen werden können. Die Nullhypothesen werden verworfen.

## 6.3 Faktoren Umwelt

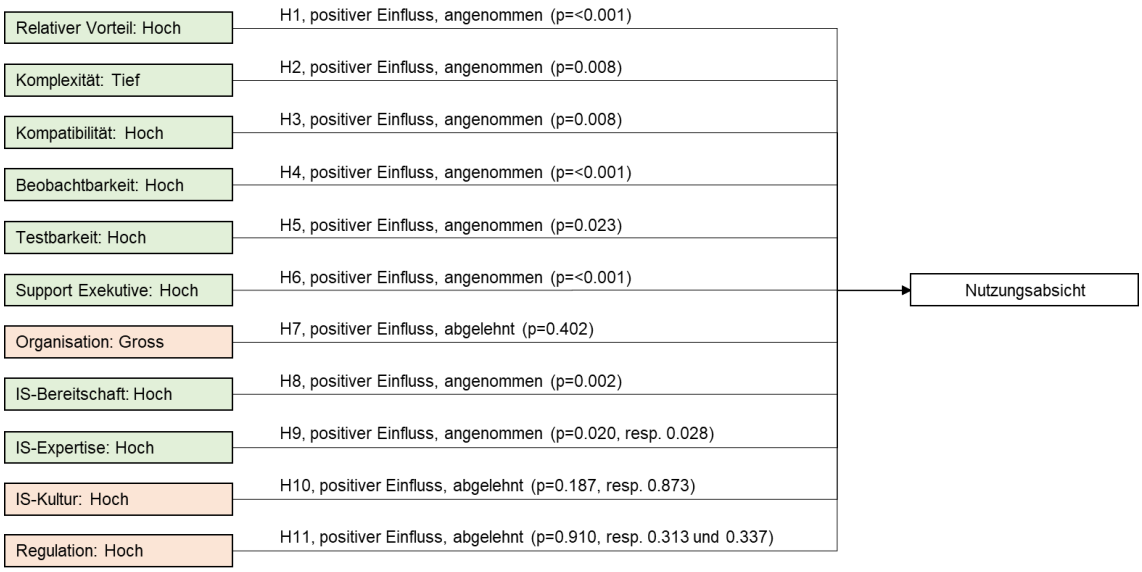
Bei den Umweltfaktoren lag der Fokus auf der Regulation. Da Gemeinden selbst gesetzgeberisch tätig sind, wurde die Regulation durch höhere Staatsebenen betrachtet. Bei den drei untersuchten Elementen Information über die Wichtigkeit, die Information über Nützlichkeit und die Förderung der Kostensenkung konnten keine signifikanten Abweichungen zwischen den Gruppen festgestellt werden. Dies widerspricht den Ergebnissen von Looi (2005, S. 71), welcher einen Einfluss dieser drei Elemente auf den Adaptionsentscheid nachgewiesen hat. Looi hat im Gegenzug zur vorliegenden Arbeit seinen Fokus auf Unternehmen gelegt. Die Adaption von Technologien im Rahmen von öffentlichen Verwaltungen unterliegt daher allenfalls anderen Faktoren.

Die Hypothese 11 (*Nutzungsabsicht ist höher, wenn die Regulation hoch ist*) wird entsprechend verworfen und die Nullhypothese angenommen.

# 7 Schlussfolgerungen und Implikationen

Von den elf aufgestellten Hypothesen müssen aufgrund der Erkenntnisse drei abgelehnt werden. Die weiteren acht Hypothesen konnten im Rahmen der Umfrage bestätigt werden. Die zusammengefassten Ergebnisse sind in Abbildung 13 dargestellt. Es zeigt sich dabei, dass bei der Organisationsgrösse, der IS-Kultur und der Regulation keine signifikanten Unterschiede festgestellt wurden. Daraus wird abgeleitet, dass zwischen diesen drei Faktoren und der der Nutzungsabsicht von BBP kein Zusammenhang besteht.

**Abbildung 13: Umgang mit Hypothesen**




*Anmerkung:* Eigene Darstellung.

Auf Basis der Ergebnisse soll die leitende Forschungsfrage inklusive der untergeordneten Forschungsfragen aus Kapitel 3.1 beantwortet werden: *Welche Voraussetzungen müssten erfüllt sein, um ein Bug-Bounty-Programm auf Ebene Gemeinde zu etablieren?*

Hierzu lässt sich festhalten, dass eine Kombination von Voraussetzungen geschaffen werden muss. Dies betrifft sowohl die Technologie von BBP als solche, wie auch organisatorische Faktoren innerhalb der Gemeindeverwaltung. Auf Seite der Technologie ist speziell eine geringe Komplexität notwendig. Die-

ser Faktor wird bei der Relevanz der Adaptionsentscheidung am höchsten gewichtet. Weiter ist ein relativer Vorteil in Bezug auf die Resultate gegenüber anderen Lösungen notwendig. Zuletzt sind die weiteren Elemente der hohen Kompatibilität, hohen Beobachtbarkeit und hohen Testbarkeit untergeordnet relevant für die Adaptionsabsicht von Gemeinden in Bezug auf innovative IS-Massnahmen wie BBP.

Bei den Organisationsfaktoren zeigt sich, dass spezifisch die Unterstützung durch die Exekutive, die IS-Bereitschaft und die IS-Expertise vorhanden sein müssen, um einen hohe Adaptionsabsicht zu provozieren. Die Grösse der Organisation und die IS-Kultur haben hingegen keinen Einfluss auf die Nutzungsabsicht von BBP. Die Regulation durch höhere Staatsebenen als einziger Umweltfaktor hat keinen Einfluss auf den Adaptionsentscheid. Bei einer Aufteilung des Faktors in die Elemente Information und Förderung konnte ebenfalls kein signifikanter Einfluss erhoben werden.

## 7.1 Implikationen für die Forschung

Im Rahmen der vorliegenden Masterarbeit konnte bestätigt werden, dass die Nutzungsabsicht von innovativen Massnahmen zur Steigerung der Informationssicherheit, konkret von Bug-Bounty-Programmen, von verschiedenen Faktoren abhängig ist. Zwar wurde die Adaption von neuen Technologien in Bezug auf die Informationssicherheit schon mehrfach untersucht, jedoch noch nie im Kontext von BBP und Gemeinden. Diese Forschungslücke konnte hiermit geschlossen werden.

Die evaluierten Faktoren sind grundsätzlich in Übereinstimmung mit der bestehenden Literatur. Trotzdem konnten Abweichungen bei den Faktoren Organisationsgrösse, IS-Kultur und Regulation festgestellt werden. Die Gründe und Abweichungen sollten hierzu verifiziert und weiter evaluiert werden. Generell bildet die vorliegende Arbeit eine erste Grundlage für die weitere Forschung in Bezug auf die Akzeptanz von innovativen Sicherheitsmassnahmen. Die Gemeinden in

der Schweiz bilden hierbei ein spannendes Forschungsobjekt, da die Entscheidungsfindung innerhalb der Organisation verschiedenen politischen, gesellschaftlichen und individuellen Einflüssen unterliegen.

## 7.2 Implikationen für die Praxis

Bug-Bounty-Programme können eine gute Massnahme zur Steigerung der Informationssicherheit darstellen. Mit der zunehmenden Digitalisierung liegt auch auf den Sicherheitsmassnahmen ein wichtiger Fokus. Jedoch wurde festgestellt, dass BBP bei den Gemeinden zu einem grossen Teil unbekannt sind. Dies betrifft insbesondere die Gemeinden aus ländlichen Gebieten und der Agglomeration. Für eine erfolgreiche Etablierung müsste daher insbesondere die Bekanntheit dieser Programme im Fokus stehen.

Gleichzeitig zeigt die Arbeit auf, welche Faktoren für den Adaptionsentscheid der Gemeinden wichtig sind. Die Komplexität gilt es hierbei als zentralen Faktor hervorzuheben. Damit ein BBP auf Ebene Gemeinde erfolgreich etabliert werden kann, muss dieses möglichst einfach in der Anwendung sein. Hohes Fachwissen darf speziell bei kleineren Gemeinden nicht vorausgesetzt werden. Zudem sollten BBP bessere Ergebnisse liefern als vergleichbare Massnahmen zur Steigerung der Informationssicherheit, damit diese vermehrt von Gemeinden adaptiert werden.

Die Cloud Security Alliance (2022, S. 8) zeigt auf, dass die Verantwortung trotz Outsourcing nicht von der Auftraggeberin an Dritte übertragen werden kann. In der vorliegenden Arbeit wird hingegen eine gegenteilige Wahrnehmung der Gemeinden offensichtlich. Durch das zunehmende Outsourcing von IT-Dienstleistungen von Gemeinden, sollten hier die rechtlichen Rahmenbedingungen und die Zuständigkeiten geklärt werden. Hierdurch werden ebenfalls indirekt die Zuständigkeiten für die Massnahmen zur Steigerung der Informationssicherheit an die entsprechenden Stellen verortet. Dies zeigt sich exemplarisch darin, dass die Gemeinden mit einem internen Verantwortungsbewusstsein stärker für das Thema sensibilisiert sind und entsprechend eine höhere Nutzungsabsicht von

BBP haben. Weitere Abklärungen in diesem Zusammenhang wären jedoch angebracht, um dies zu erörtern.

## 7.3 Limitationen und weitere Forschung

Bei der vorliegenden Arbeit wurde der Fragebogen an alle Gemeinden der Deutschschweiz verschickt. Der Entscheid, ob an der Umfrage teilgenommen wird oder nicht, lag bei der Institution selbst. Es fand keine zufallsbasierte Selektion statt, weshalb bei der Stichprobe ein Selektionsbias auftreten kann. Dasselbe gilt für die Auswahl der Person, welche die Umfrage im Namen der Gemeinde beantwortet hat. Dieser Entscheidungsprozess innerhalb der Verwaltung konnte nicht eingesehen oder beeinflusst werden.

Da die Umfrage für die Gemeinde stellvertretend durch eine Person ausgefüllt wurde, wird hierdurch allenfalls eine nicht repräsentative Haltung der Gemeinde wiedergegeben. Die Fragen wurden primär von operativ tätigen Personen beantwortet, der politische Blickwinkel fehlt hierdurch. Eine Wiederholung der Studie mit Befragung von mehreren Personen und Ebenen der Gemeinde könnte die Resultate weiter validieren.

Aufgrund des Studiendesigns lassen sich nur Korrelationen zwischen den Variablen feststellen. Die kausalen Zusammenhänge, welche effektiv zur Adaptionsabsicht führen, können hiermit nicht bestätigt werden, weshalb hierzu eine weiterführende Forschung anzustreben wäre. Durch eine vertiefte Analyse mit einer Fallstudie bei den sechs Gemeinden, welche bereits BBP eingesetzt haben, könnte dies realisiert werden.

Als Nebenprodukt konnte eine erste Bestandesaufnahme über das IT-Outsourcing bei Gemeinden der Deutschschweiz sowie deren Wahrnehmung der IS-Verantwortungsfrage erarbeitet werden. Diese Grundlage kann für weitere Forschungsarbeiten verwendet werden.

# 8 Literaturverzeichnis


Adelmeyer, M., Petrick, C., & Teuteberg, F. (2018). *IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22742-5

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Anz, P. (2021, August 30). *Cyberangriff auf Rolle: Es wird noch schlimmer*. Inside IT. https://www.inside-it.ch/post/cyberangriff-auf-rolle-es-wird-noch-schlimmer-20210830

Awa, H. O., Ojiabo, O. U., & Emecheta, B. C. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. *Journal of Science & Technology Policy Management*, *6*(1), 76–94. https://doi.org/10.1108/JSTPM-04-2014-0012

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems*, *8*(4), 244–254. https://doi.org/10.17705/1jais.00122

Baker, J. (2012). The Technology–Organization–Environment Framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Hrsg.), *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1* (Bd. 28, S. 231–245). Springer New York. https://doi.org/10.1007/978-1-4419-6108-2

Balzert, H., Schröder, M., & Schäfer, C. (2022). *Wissenschaftliches Arbeiten—Ethik, Inhalt & Form wiss. Arbeiten, Handwerkszeug, Quellen, Projektmanagement, Präsentation*. https://doi.org/10.18420/LB-WISSARBEITEN

BFS. (2016). *Die 4 Sprachgebiete der Schweiz nach Gemeinden*.

BFS. (2022a). *Ständige Wohnbevölkerung nach Alter, Kanton, Bezirk und Gemeinde, 2010-2021*.

BFS. (2022b). *Teleheimarbeit, 2001-2021*.

BFS. (2023). *Raumgliederungen am 01.01.2023*.

Bradford, M., & Florin, J. (2003). Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems. *International Journal of Accounting Information Systems*, *4*(3), 205–225. https://doi.org/10.1016/S1467-0895(03)00026-5

Bruner, G. C. (2009). *Marketing scales handbook: A compilation of multi-item measures for consumer behavior & advertising research. Volume 5* ((Library version)). GCBII Productions, LLC.

BSI. (2012). *Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter*.

BSI. (2021). *Fortschrittliche Angriffe, Neue Qualität aktueller Angriffe und Prognose*.

Buess, M., Amberg, H., & Büchler, C. (2022). *Nationale E-Government--Studie 2021. E-Government in der Schweiz aus Sicht der Bevölkerung, der Unternehmen und der Verwaltung*. Demo SCOPE AG/Interface Politikstudien Forschung Beratung GmbH.

Bundesamt für Bevölkerungsschutz. (2020). Gefährdungsdossier Cyber-Angriff. In *Katastrophen und Notlagen Schweiz 2020*.

Bundi, A. (2021, April 16). Super-GAU in Landiswil: Gemeindepräsident war «fuchsteufelswild». *BERN-OST*. https://www.bern-ost.ch/Super-GAU-in-Landiswil-Daten-verloren-Gemeindepraesident-fuchsteufelswild-637810

Cloud Security Alliance. (2022). *Top Threats to Cloud Computing*.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed). L. Erlbaum Associates.

Davis, F. D. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/15192

Deussen, P. H., Strick, L., & Peters, J. (2010). *Cloud-Computing für die öffentliche Verwaltung: ISPRAT-Studie November 2010* (1. Aufl). Frauenhofer-Inst. für Offene Kommunikationssysteme.

Digitale Verwaltung Schweiz. (2023). *Kantonale Digitalisierungsstrategien*. https://www.digitale-verwaltung-schweiz.ch/Kantonale-Digitalisierungsstrategien

ENISA. (2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.

Finanzdirektion Kanton Bern. (2021a). *Finanzstatistik der Gemeinden—Einzelauszug nach Sachgruppen—Aufwand Informatik-Unterhalt (Hardware)*.

Finanzdirektion Kanton Bern. (2021b). *Finanzstatistik der Gemeinden—Einzelauszug nach Sachgruppen—Investitionsausgaben Software*.

Fuchs, C., & Diamantopoulos, A. (2009). Using single-item measures for construct measurement in management research. *Die Betriebswirtschaft*, *69(2)*, 195–210.

Generaldirektion Informatik der Europäischen Kommission. (2019, April 5). *EU-FOSSA Bug Bounties in Full Force*. https://commission.europa.eu/news/eu-fossa-bug-bounties-full-force-2019-04-05_en

Hameed, M. A., & Arachchilage, N. A. G. (2017). *A Conceptual Model for the Organisational Adoption of Information System Security Innovations* (arXiv:1704.03867). arXiv. http://arxiv.org/abs/1704.03867

Hameed, M. A., & Counsell, S. (2014). User Acceptance Determinants of Information Technology Innovation in Organizations. *International Journal of Innovation and Technology Management*, *11*(05), 1450033. https://doi.org/10.1142/S0219877014500333

Hameed, M. A., Counsell, S., & Swift, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. *Journal of Engineering and Technology Management*, *29*(3), 358–390. https://doi.org/10.1016/j.jengtecman.2012.03.007

Horton, R. P., Buck, T., Waterson, P. E., & Clegg, C. W. (2001). Explaining Intranet use with the Technology Acceptance Model. *Journal of Information Technology*, *16*(4), 237–249. https://doi.org/10.1080/02683960110102407

Hu, P. J., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology. *Journal of Management Information Systems*, *16*(2), 91–112. https://doi.org/10.1080/07421222.1999.11518247

Hunziker, S., Portmann, A., Trachsel, V., & Dubler, F. (2022). *Cyber Risk Management in grösseren Schweizer Unternehmen*.

IBM. (2022). *Bericht über die Kosten einer Datenschutzverletzung 2022 Gesamtbericht.pdf*.

Igbaria, M., Guimaraes, T., & Davis, G. B. (1995). Testing the Determinants of Microcomputer Usage via a Structural Equation Model. *Journal of Management Information Systems*, *11*(4), 87–114. https://doi.org/10.1080/07421222.1995.11518061

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*.

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba. (2010). Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures. *Issues In Information Systems*. https://doi.org/10.48009/1_iis_2010_9-16

Jungbauer-Gans, M. (2016). *Methodische Probleme in der empirischen Organisationsforschung* (S. Liebig & W. Matiaske, Hrsg.). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-08713-5

Kantonspolizei Bern, Nationales Zentrum für Cybersicherheit (NCSC), Sicherheitsverbund Schweiz (SVS), & Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK). (o. J.). *Cyberdelikte verhindern, Wegleitung für Gemeinden*.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly*, *23*(2), 183. https://doi.org/10.2307/249751

Königs, H.-P. (2017). *IT-Risikomanagement mit System*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-12004-7

Krebs, D., & Menold, N. (2019). Gütekriterien quantitativer Sozialforschung. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 489–504). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21308-4_34

Kuehn, A., & Mueller, M. (2014). Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2418812

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, *45*(2), 109–119. https://doi.org/10.1016/j.im.2008.01.002

Looi, H. C. (2005). E-Commerce Adoption in Brunei Darussalam: A Quantitative Analysis of Factors Influencing Its Adoption. *Communications of the Association for Information Systems*, *15*. https://doi.org/10.17705/1CAIS.01503

Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, *2*(3), 173–191. https://doi.org/10.1287/isre.2.3.173

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology Special Publication 800-145*.

Microsoft Security Response Center. (2017, Juli 26). *Announcing the Windows Bounty Program*. https://msrc.microsoft.com/blog/2017/07/announcing-the-windows-bounty-program/

Min, S., So, K. K. F., & Jeong, M. (2019). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. *Journal of Travel & Tourism Marketing*, *36*(7), 770–783. https://doi.org/10.1080/10548408.2018.1507866

Mustonen-Ollila, E., & Lyytinen, K. (2003). Why organizations adopt information system process innovations: A longitudinal study using Diffusion of Innovation theory. *Information Systems Journal*, *13*(3), 275–297. https://doi.org/10.1046/j.1365-2575.2003.00141.x

Nafzger, S. (2021, April 15). *Warum die Post ein Bug Bounty Programm braucht*. https://www.post.ch/de/jobs/blog/2021/warum-die-post-ein-bug-bounty-programm-braucht

NCSC. (2021). *Abschlussbericht: Pilotprojekt «Bug Bounty-Programm der Bundesverwaltung»*.

NCSC. (2022a). *Halbjahresbericht 2022/I (Januar – Juni)*.

NCSC. (2022b). *Q&A Bug-Bounty-Programm der Bundesverwaltung*.

NCSC. (2022c, Oktober 14). *Schützen Sie Ihre Behörde*. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/aktuelle-themen/schuetzen-sie-ihre-behoerde.html

NCSC. (2022d, Dezember 8). *Ransomware*. https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/ransomware.html

Neumann, P. (2013). *Handbuch der psychologischen Marktforschung: Stichprobenauswahl - Forschungsstrategien - qualitative und quantitative Methoden - Auswertung und Visualisierung der Daten - Präsentation der Ergebnisse* (1. Aufl). Huber.

Oliveira, T., & Martins, M. F. (2011). *Literature Review of Information Technology Adoption Models at Firm Level*.

Pan, M.-J., & Jang, W.-Y. (2008). Determinants of the Adoption of Enterprise Resource Planning within the Technology-Organization-Envi. *Journal of Computer Information Systems*.

Paresh, D. (2017, Oktober 19). *Google offers bug bounty to clean up mobile apps*. https://www.reuters.com/article/ctech-us-alphabet-google-cyber-bounty-idCAKBN1CO2RI-OCATC

Premkumar, G., Ramamurthy, K., & Nilakanta, S. (1994). Implementation of Electronic Data Interchange: An Innovation Diffusion Perspective. *Journal of Management Information Systems*, *11*(2), 157–186. https://doi.org/10.1080/07421222.1994.11518044

Rasch, B., Friese, M., Hofmann, W., & Naumann, E. (2008). *Quantitative Methoden* (2., erw. Aufl., korr. Nachdr). Springer Medizin Verl.

Regierungsrat Kanton Basel-Stadt. (2021). *Regierungsratsbeschluss vom 19. Oktober 2021 Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Stellungnahme des Kantons Basel-Stadt*.

Regierungsrat Kanton Zürich. (2021). *Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (Vernehmlassung)*.

Röbken, H., & Wetzel, K. (2016). *Qualitative und quantitative Forschungsmethoden*.

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed). Free Press ; Collier Macmillan.

Rohlfs, T., & Mahnke, A. (2020). Risikomanagement im Unternehmen. In *Betriebliches Risikomanagement und Industrieversicherung: Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement* (S. 3–16). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-30421-8

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Salleh, K. A., & Janczewski, L. (2016). *Adoption of Big Data Solutions: A study on its security determinants using Sec-TOE Framework*.

Schläger, U., & Thode, J.-C. (2022). *Handbuch Datenschutz und IT-Sicherheit*. Erich Schmidt Verlag GmbH & Co. KG. https://doi.org/10.37307/b.978-3-503-20534-9

Schürmann, F. (2018). Cloud Security. In *Ausgewählte Aspekte des Cloud-Computing aus einer IT-Management-Perspektive*. DuEPublico: Duisburg-Essen Publications Online, University of Duisburg-Essen, Germany. https://doi.org/10.17185/DUEPUBLICO/47077

Schweizer Bundesrat. (2020). *Botschaft zur Legislaturplanung 2019–2023*.

Skorna, A., & Nießen, P. (2020). Risikoanalyse, -bewertung und -steuerung. In A. Mahnke & T. Rohlfs (Hrsg.), *Betriebliches Risikomanagement und Industrieversicherung: Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement* (S. 41–65). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-30421-8

Staatskanzlei Kanton Bern. (2023a). *Gesetz über die digitale Verwaltung tritt in Kraft*. https://www.sta.be.ch/de/start/themen/digitale-verwaltung.html?newsID=2e4ff5fd-d2ff-43cf-867b-4190697fe2a3

Staatskanzlei Kanton Bern. (2023b). *Strategie Digitale Verwaltung des Kantons Bern*.

Stein, P. (2019). Forschungsdesigns für die quantitative Sozialforschung. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 125–142). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21308-4_8

Steiner, R., Ladner, A., Kaiser, C., Haus, A., Amsellem, A., & Keuffer, N. (2021). *Zustand und Entwicklung der Schweizer Gemeinden: Ergebnisse des nationalen Gemeindemonitorings 2017* [176,application/pdf]. Somedia Buchverlag. https://doi.org/10.21256/ZHAW-3134

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

United Nations. (2022). *United Nations E-Government survey 2022: The future of digital government*.

US Department of Defence. (2016). *"Hack the Pentagon" Fact Sheet*.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Walshe, T., & Simpson, A. (2020). An Empirical Study of Bug Bounty Programs. *2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*, 35–44. https://doi.org/10.1109/IBF50092.2020.9034828

Walz, A., Klemens, J., & Röpke, R. (2020). Cyber: Cyber-Risiken, eine wachsende Bedrohung. In A. Mahnke & T. Rohlfs (Hrsg.), *Betriebliches Risikomanagement und Industrieversicherung: Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement* (S. 447–469). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-30421-8

Wang, Y.-M., Wang, Y.-S., & Yang, Y.-F. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. *Technological Forecasting and Social Change*, *77*(5), 803–815. https://doi.org/10.1016/j.techfore.2010.03.006

YesWeHack. (2023). *SWISS POST - E-VOTING*. https://yeswehack.com/programs/swiss-post-evoting

# 9 Anhang

## 9.1 Fragebogen

Guten Tag. Vielen Dank, dass Sie sich die Zeit für die Umfrage zum Thema Informationssicherheit in Gemeinden nehmen. Die Umfrage umfasst maximal 30 Fragen und nimmt ca. 20 Minuten in Anspruch. Ihre Daten werden anonym erhoben und ausschliesslich für die Forschungsarbeit im Rahmen der Masterthesis verwendet.

**1 - Eine Möglichkeit zur Förderung der Informationssicherheit (Cybersecurity) von Organisationen sind sogenannte Bug-Bounty-Programme. Wissen Sie, worum es sich dabei handelt?**

◯ Ja

◯ Nein

**Sofern 1 Ja: 2 - Erklären Sie bitte kurz, was ein Bug Bounty Programm ist.**

_____

**Sofern 1 Ja: 3 - Hat Ihre Gemeinde bereits an einem Bug-Bounty-Programm teilgenommen oder selbst durchgeführt?**

◯ Ja

◯ Nein

**4 - Bug-Bounty-Programme**

Der Bund definiert Bug-Bounty-Programme wie folgt: Die Programme dienen dazu, in Zusammenarbeit mit ethischen Hackern allfällige Verwundbarkeiten in IT-Systemen zu identifizieren, zu dokumentieren und zu beheben. Ethische Hacker, oder Hacker mit guten Absichten, sind Sicherheitsexperten, die IT-Systeme und Produkte im Auftrag prüfen. Dabei suchen sie nach Schwachstellen, die auch Hacker mit bösartigen Absichten ausnutzen könnten. Die Hacker nutzen eigene Methoden, um Schwachstellen zu identifizieren, welche mit klassischen Penetrationstests oder Security Reviews nicht immer gefunden werden können. Bei dieser Schwachstellen-Suche halten sich die ethischen Hacker an einen vordefinierten Rahmen, welcher im Bug-Bounty-Programm festgelegt wird. Finden ethische Hacker eine Schwachstelle, melden sie diese und nutzen sie nicht zu ihrem eigenen Vorteil aus. Für gefundene Schwachstellen wird eine Belohnung (Bounty) ausbezahlt. Die Höhe der Belohnung richtet sich nach der Schwere der gefundenen Lücke. In der Regel betragen die Belohnungen für einen leichten Sicherheitsverstoss zwischen CHF 500 bis CHF 1'000.

Bug-Bounty-Programme können sowohl von Organisationen selbst durchgeführt werden oder die Dienstleistung wird von einer Plattform bezogen.

**5 - Können Sie sich vorstellen, dass Ihre Gemeinde in Zukunft an einem Bug-Bounty-Programm teilnehmen wird?**

◯ Ja

◯ Nein

**6 - Wie beurteilen Sie folgende Aussage: Unsere Gemeindeexekutive unterstützt den Einsatz von innovativen Massnahmen (z. B. Bug-Bounty-Programmen) zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu

◯ 6 - stimme zu

◯ 5 - stimme eher zu

◯ 4 - neutral

◯ 3 - stimme eher nicht zu

◯ 2 - stimme nicht zu

◯ 1 - stimme überhaupt nicht zu

**7 - Wie hoch schätzen Sie die potenzielle Bedrohungslage der Informationssicherheit für Ihre Gemeinde ein?**

◯ 7 - sehr hoch

◯ 6 - hoch

◯ 5 - eher hoch

◯ 4 - neutral

◯ 3 - eher tief

◯ 2 - tief

◯ 1 - sehr tief

**8 - Wie hoch schätzen Sie die Erfahrung Ihrer Gemeinde in Bezug auf das Erkennen und Bewerten von Bedrohungen der Informationssicherheit ein?**

◯ 7 - sehr hoch
◯ 6 - hoch
◯ 5 - eher hoch
◯ 4 - neutral
◯ 3 - eher tief
◯ 2 - tief
◯ 1 - sehr tief

**9 - Wie hoch sind Ihre personellen Ressourcen für den Einsatz von innovativen Massnahmen zur Erhöhung der Informationssicherheit?**

◯ 7 - sehr hoch
◯ 6 - hoch
◯ 5 - eher hoch
◯ 4 - neutral
◯ 3 - eher tief
◯ 2 - tief
◯ 1 - sehr tief

**10 - Sind Massnahmen zur Steigerung der Informationssicherheit bei den Mitarbeitenden allgemein akzeptiert?**

◯ 7 - sehr akzeptiert
◯ 6 - akzeptiert
◯ 5 - eher akzeptiert
◯ 4 - neutral
◯ 3 - eher nicht akzeptiert
◯ 2 - nicht akzeptiert
◯ 1 - völlig nicht akzeptiert

**11 - Wie schätzen Sie das Bewusstsein der Mitarbeitenden in Ihrer Gemeinde in Sachen Informationssicherheit ein?**

◯ 7 - sehr hohes Bewusstsein
◯ 6 - hohes Bewusstsein
◯ 5 - eher hohes Bewusstsein
◯ 4 - neutral
◯ 3 - eher tiefes Bewusstsein
◯ 2 - tiefes Bewusstsein
◯ 1 - sehr tiefes Bewusstsein

**12 - Technologische Aspekte**

Nachfolgende Fragen beziehen sich auf Ihre Nutzungsabsicht in Bezug auf neue und innovative Sicherheitsmassnahmen zur Erhöhung der Informationssicherheit, zum Beispiel die eingangs erwähnten Bug-Bounty-Programme. Bitte beurteilen Sie die nachfolgenden Aussagen:

**13 - Wir nutzen neue und innovative Massnahmen zur Erhöhung der Informationssicherheit, sofern die neuen Massnahmen bessere Ergebnisse erzielen als die heutigen Hilfsmittel.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**14 - Sofern es eine kostengünstige Methode zur Identifikation von Sicherheitslücken darstellt, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**15 - Sofern deren Nutzung einfach ist, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**16 - Sofern die Methode / das Produkt zu unseren Wertvorstellungen passt, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**17 - Sofern die Resultate gut beobachtbar sind, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**18 - Sofern die Technik vor der definitiven Einführung getestet werden kann, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**19 - Optionaler Kommentar**

_____

**20 - Umweltfaktoren**

Bitte beurteilen Sie die nachfolgenden Aussagen:

**21 - Die höheren Staatsebenen (Bund, Kanton) informieren über die Wichtigkeit von innovativen Massnahmen zur Steigerung Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**22 - Die höheren Staatsebenen (Bund, Kanton) informieren über die Nützlichkeit von innovativen Massnahmen zur Steigerung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**23 - Die höheren Staatsebenen (Bund, Kanton) unterstützen die Senkung der Kosten durch den Einsatz von innovativen Massnahmen zur Steigerung der Informationssicherheit.**

◯ 7 - stimme völlig zu
◯ 6 - stimme zu
◯ 5 - stimme eher zu
◯ 4 - neutral
◯ 3 - stimme eher nicht zu
◯ 2 - stimme nicht zu
◯ 1 - stimme überhaupt nicht zu

**24 - Optionaler Kommentar**

_____

**25 - Welche der vorgängig erwähnten Faktoren ist aus Ihrer Sicht für die Nutzung von innovativen Massnahmen zur Erhöhung der Informationssicherheit am relevantesten? Mehrfachauswahl möglich.**

☐ Bessere Ergebnisse als vergleichbare Hilfsmittel
☐ Kostengünstiger als andere Massnahmen
☐ Einfache Nutzung
☐ Übereinstimmung mit Wertevorstellungen
☐ Beobachtbarkeit von Resultaten
☐ Testbarkeit bevor definitiver Einführung
☐ Information durch übergeordnete Staatsebenen (Bund, Kanton)
☐ Unterstützung / Förderung durch übergeordnete Staatsebenen (Bund, Kanton)

Andere (bitte ergänzen)

_____

Optionaler Kommentar

_____

**26 - Wie beurteilen Sie die Erfüllung der nachfolgenden Faktoren in Bezug auf Bug-Bounty-Programme (BBP)?**

1 Stern = überhaupt nicht erfüllt

7 Sterne = vollständig erfüllt

BBP liefern bessere Ergebnisse als vergleichbare Hilfsmittel (z. B. Penetrationstest)

BBP sind kostengünstiger als andere Massnahmen

BBP sind einfach in der Nutzung

BBP passen zu unseren Wertevorstellungen

Resultate von BBP sind gut beobachtbar

BBP lassen sich vorgängig gut testen

Übergeordnete Staatsebenen (Bund, Kanton) informieren über BBP

Übergeordnete Staatsebenen (Bund, Kanton) unterstützen BBP

**27 - Wie viele Einwohnerinnen und Einwohner zählt Ihre Gemeinde?**

◯ 100 000 und mehr Einwohner/innen

◯ 50 000 - 99 999 Einwohner/innen

◯ 20 000 - 49 999 Einwohner/innen

◯ 10 000 - 19 999 Einwohner/innen

◯ 5 000 - 9 999 Einwohner/innen

◯ 2 000 - 4 999 Einwohner/innen

◯ 1 000 - 1 999 Einwohner/innen

◯ weniger als 1 000 Einwohner/innen

**28 - Wie viele Mitarbeitende beschäftigt Ihre Gemeinde in der Verwaltung?**

◯ 1 - 4

◯ 5 - 9

◯ 10 - 19

◯ 20 - 49

◯ 50 - 99

◯ 100 und mehr

**29 - Zu welcher Kategorie zählen Sie Ihre Gemeinde?**

◯ Urbane Gemeinde

◯ Agglomerationsgemeinde

◯ Ländliche Gemeinde

**30 - Haben Sie Ihre Informatik oder Teile davon ausgelagert?**

◯ Nein, die Informatik wird intern bereitgestellt.

◯ Ja, die Informatik ist teilweise ausgelagert.

◯ Ja, die Informatik ist vollständig ausgelagert.

◯ Keine Angabe.

**31 - Wer trägt Ihrer Meinung nach bei einem Datenverlust die Verantwortung?**

◯ Exekutive

◯ Zuständige Abteilung

◯ Externer Dienstleister

**32 - Welche Funktion üben Sie aus?**

◯ Mitglied der Exekutive

◯ Leiter:in Informatik

◯ Finanzverwalter:in

◯ Gemeindeschreiber:in

Andere

_____

**33 - Haben Sie noch eine abschliessende Bemerkung zum Thema?**

_____

34 - Vielen Dank für Ihre Zeit und das Ausfüllen des Fragebogens. Falls Sie an den Ergebnissen der Arbeit interessiert sind, können Sie nachfolgend freiwillig Ihre E-Mail-Adresse hinterlegen. Ihre E-Mail-Adresse wird ausschliesslich für den Versand der Thesis genutzt. Die Ergebnisse werden voraussichtlich Ende Sommer 2023 publiziert.

35 - Wenn Sie an der freiwilligen Verlosung teilnehmen möchten, geben Sie bitte Ihre E-Mail-Adresse an. Unter allen Eingaben werden drei Thuner Spezialitätenboxen verlost. Ihre E-Mail-Adresse wird ausschliesslich für die Verlosung und die Kontaktaufnahme in diesem Zusammenhang genutzt.

## 9.2 Operationalisierung unabhängige Variablen

| Variable | Frage | Quelle |
|---|---|---|
| Support Exekutive | Unsere Gemeindeexekutive unterstützt den Einsatz von innovativen Massnahmen (z. B. Bug-Bounty-Programmen) zur Erhöhung der Informationssicherheit. | Salleh und Janczewski (2016, S. 9) |
| IS-Expertise | Wie hoch schätzen Sie die potenzielle Bedrohung der Informationssicherheit für Ihre Gemeinde ein? | Safa et al. (2015, S. 73) |
| IS-Expertise | Wie hoch schätzen Sie die Erfahrung Ihrer Gemeinde in Bezug auf das Erkennen und Bewerten von Bedrohungen der Informationssicherheit ein? | Safa et al. (2015, S. 73) |
| IS-Bereitschaft | Wie hoch sind Ihre personellen Ressourcen für den Einsatz von innovativen Massnahmen zur Erhöhung der Informationssicherheit? | Safa et al. (2015, S. 73) |
| IS-Kultur | Sind Massnahmen zur Steigerung der Informationssicherheit in Ihrer Gemeinde allgemein akzeptiert? | Salleh und Janczewski (2016, S. 9) |
| IS-Kultur | Wie schätzen Sie das Bewusstsein der Mitarbeitenden in Ihrer Gemeinde in Sachen Informationssicherheit ein? | Salleh und Janczewski (2016, S. 9) |
| Relativer Vorteil | Sofern die Sicherheit unserer Informatiksysteme verbessert wird, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |
| Relativer Vorteil | Sofern es eine kostengünstige Methode zur Identifikation von Sicherheitslücken darstellt, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |

| | | |
|---|---|---|
| Komplexität | Sofern die Nutzung einfach ist, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |
| Kompatibilität | Sofern es zu unseren Wertvorstellungen passt, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |
| Beobachtbarkeit | Sofern die Resultate gut beobachtbar sind, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |
| Testbarkeit | Sofern es vor der definitiven Einführung getestet werden kann, nutzen wir neue und innovative Massnahmen zur Erhöhung der Informationssicherheit. | Lee und Kozar (2008, S. 117) |
| Regulation | Die höheren Staatsebenen (Bund, Kanton) informieren über die Wichtigkeit von innovativen Massnahmen zur Steigerung Informationssicherheit. | Looi (2005, S. 68) |
| Regulation | Die höheren Staatsebenen (Bund, Kanton) informieren über die Nützlichkeit von innovativen Massnahmen zur Steigerung der Informationssicherheit. | Looi (2005, S. 68) |
| Regulation | Die höheren Staatsebenen (Bund, Kanton) unterstützen die Senkung der Kosten durch den Einsatz von innovativen Massnahmen zur Steigerung der Informationssicherheit. | Looi (2005, S. 68) |
| Organisations-grösse | Wie viele Mitarbeitende beschäftigt die Gemeinde in der Verwaltung? | - |