FERDINAND PORSCHE
FERN FH

E-Commerce & IT-Sicherheit

Status quo, Nutzerverhalten und Ausblick auf die Zukunft

Masterarbeit

eingereicht von: Thomas Trillsam, BSc
Matrikelnummer: 1510471046

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH Gesellschaft zur Erhaltung und Durchführung von Fachhochschul-Studiengängen

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Mag. Reinhard Neubauer

Zweitgutachten: DI Thomas Györgyfalvay, B.A., MBA

Wiener Neustadt, Mai 2017

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.

2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, 31.05.2017 _____

Unterschrift

Kurzzusammenfassung: E-Commerce & IT-Sicherheit: Status quo, Nutzerverhalten und Ausblick auf die Zukunft

Diese Arbeit beschäftigt sich mit dem Einfluss der IT-Sicherheit und deren Methoden auf das Nutzerverhalten von Konsumierenden im Rahmen des E-Commerce. Neben der Forschungsfrage wird die Hypothese vorangestellt, dass die tatsächlichen Auswirkungen auf das Nutzerverhalten trotz ständiger Weiterentwicklung der Sicherheitstechnologien als gering anzusehen sind. Durch eine ausführliche Literaturrecherche werden relevante Begriffe sowie der Status quo ausführlich erhoben. Mittels einer quantitativen Online-Umfrage unter Selbstselektion wurden in weiterer Folge Daten für eine anschließende Analyse gesammelt. Das Ergebnis dieser Arbeit zeigt eine Bestätigung der Hypothese, wonach Defizite in Bezug auf die Kenntnisse der Nutzer sowie eine hohe Diskrepanz zwischen der Selbsteinschätzung und der tatsächlich erzielten Sicherheit festgestellt werden können. Weiters kann bestätigt werden, dass IT-Sicherheitsmaßnahmen im Bereich des E-Commerce weitestgehend falsch interpretiert werden. Der Ausblick auf die Zukunft zeigt hohes Potential im Bereich der autonomen Sicherheitstechnologien sowie der Nutzerwahrnehmung.

Schlagwörter:

IT-Sicherheit, Empirie, Sicherheitstechnologien, Nutzerverhalten, Nutzerwahrnehmung, E-Commerce, Konsumierende, Fragebogen

Abstract: E-Commerce & IT Security: Status quo, user behavior and outlook

The present paper deals with the influence of IT security and commonly used methods and how they impact pattern of use in e-commerce and therefore perception of customers. The scientific problem revolves around a hypothesis under the assumption of a generally low impact in relation to user behavior, despite the fact of rising technologies and functionalities. To present a comprehensive overview of the state of science, the status quo of currently used methods and their impact on users is being elaborated through a detailed literature research. Empirical evidence has been collected through an online questionnaire. The result of this study shows the confirmation of the hypothesis in IT security mechanics having low impact on users in general. It further

shows the lack of knowledge on this area of field, which also yields in poor self-assessments. Future studies are advised to do research either in the field of user perception and how to influence self-awareness or focus on improved technologies to eliminate human error and failure in addition of fixing potential unawareness of IT security threats.

Inhaltsverzeichnis

1. Einleitung

1.1. Hintergrund und Problemstellung

Aktuelle technologische Entwicklungen im Bereich der IT-Sicherheit haben direkte Auswirkungen auf den Bereich des E-Commerce und damit auch auf die Nutzer selbst. Die Schwierigkeit liegt in der Überprüfung und Anwendung seitens der konsumierenden Zielgruppe. Zahlreiche Methoden wie beispielsweise Browser Plugins und Funktionalitäten versuchen, den Nutzer über wichtige Merkmale der jeweils aktiven Verbindung und der verwendeten Zertifikate, Cookies und Verschlüsselungssysteme zu informieren. Genau hier liegt die Schwierigkeit, nämlich IT-Sicherheit transparent und für die Anwendenden verständlich und nachvollziehbar aufzubereiten. Trotz immer fortschrittlicher Technologie und ständiger Weiterentwicklung kommt es im Alltag zu regelmäßigen Sicherheitsvorfällen. Ausgehend von dieser Problemstellung sollen Zusammenhänge zwischen IT-Sicherheit und Nutzerverhalten erforscht, und damit die im folgenden Kapitel formulierte Forschungsfrage beantwortet werden.

1.2. Forschungsfrage

Ziel dieser Arbeit ist es, den Zusammenhang zwischen IT-Sicherheit, dem technologischen Fortschritt und dessen Entwicklungen sowie der tatsächlichen Nutzerwahrnehmung und Risikoeinschätzung, zu erforschen. Die Forschungsfrage lautet daher, inwiefern IT-Sicherheit das Nutzerverhalten von Konsumierenden im Rahmen des E-Commerce beeinflusst. Um diese Frage zu beantworten, soll im empirischen Teil durch die Verwendung eines Fragebogens eine umfangreiche Datenanalyse durchgeführt werden. Dadurch soll die im Rahmen dieser Arbeit aufgestellte Hypothese auf Gültigkeit überprüft werden. Die Hypothese unterstellt geringe Auswirkungen auf das Nutzerverhalten, obwohl eine ständige Weiterentwicklung der verwendeten Sicherheitstechnologien beobachtet werden kann.

1.3. Methodik

Im ersten Teil dieser Arbeit wird hauptsächlich auf wissenschaftliche Literatur zurückgegriffen. Eine ausführliche Recherche zu den Themen IT-Sicherheit, Risikowahrnehmung sowie den Vor- und Nachteilen von E-Commerce soll Aufschluss über den Status quo und aktuelle Entwicklungen geben. Der zweite Teil dieser Arbeit stellt die Erhebung statistischer Daten dar, dies soll in Form einer quantitativen Online-Erhebung mittels Fragebogen und unter Selbstselektion durchgeführt werden. Anschließend werden die gesammelten Daten ausgewertet, und relevante Zusammenhänge diskutiert. Im Zuge dessen soll die Hypothese dieser Studie bestätigt oder verworfen werden. Das Ende dieser Arbeit bildet eine Zusammenfassung der wichtigsten Erkenntnisse und Schlussfolgerungen sowie ein Ausblick auf die Zukunft.

2. Theoretische Grundlagen

Dieses und das darauffolgende Kapitel stellen den theoretischen Teil dieser Arbeit dar, welcher die Grundlage für den empirischen Teil bildet. Während im ersten Teil verstärkt auf Begriffsdefinitionen und grundlegende Zusammenhänge zwischen IT-Sicherheit sowie den daraus folgenden Bedrohungen und Schutzzielen eingegangen wird, werden in Kapitel 3 konkrete E-Commerce relevante Risiken sowie zugehörige IT-Sicherheitsmaßnahmen vorgestellt.
In diesem Kapitel sollen zunächst die wichtigsten Begriffe im Zusammenhang mit IT-Sicherheit und E-Commerce erläutert werden.

2.1. IT-Sicherheit

Der Begriff der IT-Sicherheit lässt sich nicht als statisches Betrachtungsobjekt definieren. Vielmehr unterliegt die IT-Sicherheit einem stetigen Wandel unter Berücksichtigung der technologischen Entwicklungen und dem Gefahrenpotential. Des Weiteren teilt sich der Begriff der IT-Sicherheit auf verschiedene Teilaspekte auf. Diese Teilaspekte umfassen auch den physikalischen Schutz, also den Schutz vor physischem Zugang zu Informationssystemen. Ganzheitlich lässt sich der Begriff der IT-Sicherheit daher als dynamisches Objekt darstellen.[1]
Nachfolgend eine von vielen möglichen Definitionen von IT-Sicherheit, nach dem Online-Lexikon für Informationstechnologie:

> *„Die IT-Sicherheit tangiert alle technischen Maßnahmen zur Verringerung des Gefährdungspotenzials für IT-Anwendungen und -Systeme. Alle mit dem Gefährdungspotenzial in Zusammenhang stehenden Schutzmaßnahmen, wie die Entwicklung von Sicherheitskonzepten, die Vergabe von Zugriffsberechtigungen und die Implementierung von Sicherheitsstandards, sind Aspekte der*

[1] Vgl. Enzyklopädie der Wirtschaftsinformatik, URL: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html (abgerufen am 14.12.2016), Universität Potsdam, Potsdam, 2016

> *IT-Sicherheit. IT-Sicherheit ist die technische Umsetzung der Sicherheitskonzepte unter wirtschaftlichen Aspekten."*[2]

Dies bedeutet in weiterer Folge, dass der Fokus zunächst auf die Erfassung der schützenswerten Systeme, Einrichtungen und Personen gelegt werden muss. Dies entspricht in der Praxis zunächst dem Informationssystem selbst. Aber auch Personen, welche mit dem System in Berührung kommen, externe Institutionen oder Beteiligte sowie die eingesetzte Software sind Bestandteil der IT-Sicherheit. Um diesen Vorgang zu vereinfachen, werden in der Regel Schutzziele definiert.[3]

Der Bereich der IT-Sicherheit wird auch synonym für weitere Begriffe genannt, wie beispielsweise Cyber Security oder Informationssicherheit. Je nach Literatur – und vor allem im deutschen Sprachgebrauch – kommt es oft zu einer differenzierten Betrachtungsweise bezüglich der genauen Definition dieser Begriffe. So wird der Begriff Cyber Security oftmals als Überbegriff genannt. Hierzu zählen sämtliche Bedrohungen und auch Risiken, welche in den Bereich der IT fallen. Darunter unter anderem die gesamte Sicherheitsarchitektur, die sichere Authentifikation und Zugriffskontrolle, die Sicherheit in IT-Netzen bis hin zu den Themen Datenschutz und Notfallplanung. In der Regel finden sich Spezialisten eines oder mehrerer Teilgebiete, jedoch immer aufgeteilt auf verschiedene Personen. Auch eine Verschmelzung zwischen verschiedenen Fachbereichen lässt sich beobachten, wie zum Beispiel auf dem Gebiet der Rechtswissenschaften.[4]

Die verschiedenen Bedrohungen in Bezug auf IT-Sicherheit sowie die entsprechenden Schutzziele und ihre Definitionen werden in den beiden nachfolgenden Kapiteln näher erläutert.

---

[2] Das große Online-Lexikon für Informationstechnologie, URL: http://www.itwissen.info/definition/lexikon/IT-Sicherheit-IT-security.html (abgerufen am 14.12.2016), DATACOM Buchverlag GmbH, Peterskirchen, 2016

[3] Vgl. Das große Online-Lexikon für Informationstechnologie, 2016

[4] Vgl. Klipper, S.: Cyber Security: Ein Einblick für Wirtschaftswissenschaftler, Wiesbaden, 2015, S5f

2.2. Bedrohungen

Die IT in ihrer aktuellen Form bietet eine große Angriffsfläche für eine Vielzahl von Bedrohungen. Vor allem die Vernetzung der verschiedenen Geräte und Portale und deren ständige Kommunikation lässt vielfältige Angriffsszenarien zu. Neben dem Desktop als Hauptrechner werden auch Tablets, Smartphones bis hin zu Fernsehgeräten und E-Book Readern als Einstieg in zahlreiche E-Commerce Prozesse genutzt. Dadurch ergeben sich für den Bereich der IT-Sicherheit immer wieder neue Gefahren, welche aus Nutzersicht nicht in allen Fällen als solche erkannt werden (vgl. Abbildung 1).[5]

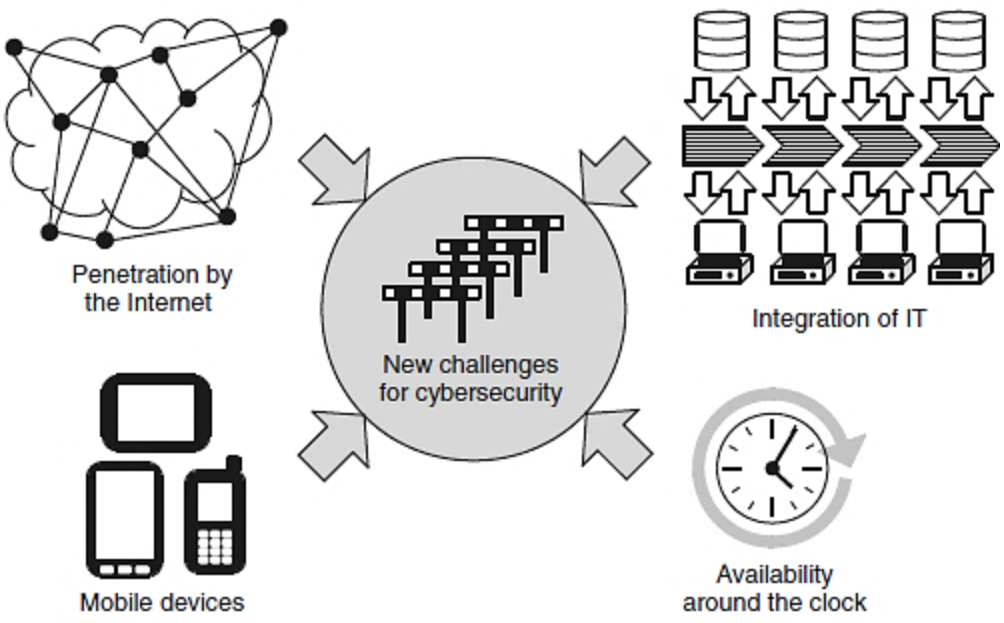


Abbildung 1: Neue Herausforderungen für die IT-Sicherheit[6]

Nachfolgend soll auf jede dieser Herausforderungen näher eingegangen werden. Ergänzend der Hinweis auf die Existenz von weiteren Bedrohungen sowie auch

[5] Vgl. Beissel, S.: Cybersecurity Investments: Decision Support Under Economic Aspects, International Publishing Switzerland, 2016, S1ff

[6] Abbildung entnommen aus: Beissel, S.: Cybersecurity Investments, S3

Untergruppen der in Abbildung 1 angegebenen Themen. Die vier behandelten Themen stellen jedoch die Eckpfeiler der modernen Herausforderungen an die IT-Sicherheit dar.[7]

2.2.1. Internet

In der heutigen Zeit wird eine Vielzahl von internetfähigen Endgeräten eingesetzt. Neben den bereits in Kapitel 2.2. aufgezählten Geräten, bauen mittlerweile auch Haushaltsgeräte, Uhren (sogenannte „Smart Watches“) bis hin zum Media Center oder der Außenkamera eine stetige Internetverbindung auf. Dies führt zu einem beträchtlichen Sicherheitsrisiko, da die verschiedenen Einstiegspunkte für Angreifende immer vielfältiger werden. Sie haben die Wahl zwischen vielen verschiedenen Systemen, welche unterschiedlich gut abgesichert sind. Die Angreifenden suchen sich daher das schwächste Glied in der Kette aus. Auch die Wahrscheinlichkeit, ein unzureichend abgesichertes System zu finden, liegt deutlich höher als in der Vergangenheit.

Als weiterer Punkt kann das Sammeln von Informationen im Zusammenhang mit diesen vernetzten Endgeräten angeführt werden. Die Kombination aus der Datenspeicherung von beispielsweise Bewegungsdaten und der Vernetzung mit dem Internet stellt für Eindringlinge ein lukratives Ziel dar.[8]

2.2.2. Integration der IT

Die Integration der IT in die Prozesse und Workflows führt für Unternehmen und Konzerne zumeist zu einer deutlichen Effektivitäts- und in weiterer Folge zu einer Umsatzsteigerung. Abläufe können durch eine umfangreiche und sorgfältig geplante Integration der IT entscheidend beschleunigt und optimiert werden. In diesem Zusammenhang nimmt vor allem die Cloud eine entscheidende Rolle ein. Der Schlüssel zum sinnvollen Einsatz der Cloud liegt in der Nutzung als Service. Sobald ein Prozess erfolgreich als Service innerhalb der Cloud etabliert wird, können Beschäftigte und Nutzer von nahezu jedem internetfähigen Gerät auf dieses zugreifen. Auch die Verarbeitung der gesammelten Daten lässt sich vereinfachen.[9]

---

[7] Vgl. Beissel, S.: Cybersecurity Investments, S2

[8] Vgl. Beissel, S.: Cybersecurity Investments, S2ff

[9] Vgl. Beissel, S.: Cybersecurity Investments, S3f

Als weiterer Punkt lässt sich die Komplexität der verschiedenen Systeme anführen. Die reine Anzahl der verfügbaren Komponenten, welche miteinander vernetzt sind, führt zu einer gewissen Unübersichtlichkeit und damit auch zu einer potentiell unbemerkten Schwachstelle.[10]

2.2.3. Mobile Geräte

Der Ausbau der stetigen Vernetzung von diversen Endgeräten lässt sich vor allem im Bereich der mobilen Geräte beobachten. Vor allem die Verwendung von Smartphones und Tablets führt zu einer immer größer werdenden Nachfrage. Dies wiederum führt zu einem unaufhaltsamen Strom an neuen Apps und Produkten, die diese Plattformen bedienen. Als Ergebnis gestaltet sich die Entwicklung von Viren, Spyware und anderen schadhaften Programmen für Angreifende als sehr lukrativ. Mit dem nicht enden wollenden Wachstum im mobilen Bereich kommt es zu einer weiteren Zunahme von Bedrohungen im E-Commerce.[11]

2.2.4. Verfügbarkeit

Als logische Folge aus der Verwendung von mobilen Geräten und einer wachsenden Vernetzungs- und Kommunikationsrate wird von IT-Systemen eine ständige Verfügbarkeit verlangt. Dies lässt sich auch anhand der steigenden Verfügbarkeit der mit diesen Systemen verbundenen Personen, seien es nun Beschäftigte oder Privatpersonen, beobachten. Im Bereich der IT-Sicherheit ist dieser Umstand von großem Vorteil, da eine ausgedehnte Verfügbarkeit das Fenster für Angriffe öffnet und ein erfolgreicher Angriff schneller ausgeführt werden kann. Auch die Zeiten der Inaktivität der Nutzer entsprechen Zeiten in welchen dennoch eine aufrechte Internet- und Kommunikationsverbindung besteht, und stellen demnach ein Sicherheitsrisiko dar.[12]

[10] Vgl. Beissel, S.: Cybersecurity Investments, S3f

[11] Vgl. Beissel, S.: Cybersecurity Investments, S3f

[12] Vgl. Beissel, S.: Cybersecurity Investments, S3f

2.3. Schutzziele

Schutzziele werden in der Literatur in den Kern und die Gruppe der weiteren Schutzziele aufgeteilt. Während der Kern bereits eine abgeschlossene Liste darstellt, werden weitere Schutzziele definiert, welche damit verwandte aber zumeist auf konkrete Anwendungsfälle abgezielte Themen behandeln. Zusammen bilden sie den gesamten Pool der Schutzziele in der IT-Sicherheit (vgl. Abbildung 2).[13]

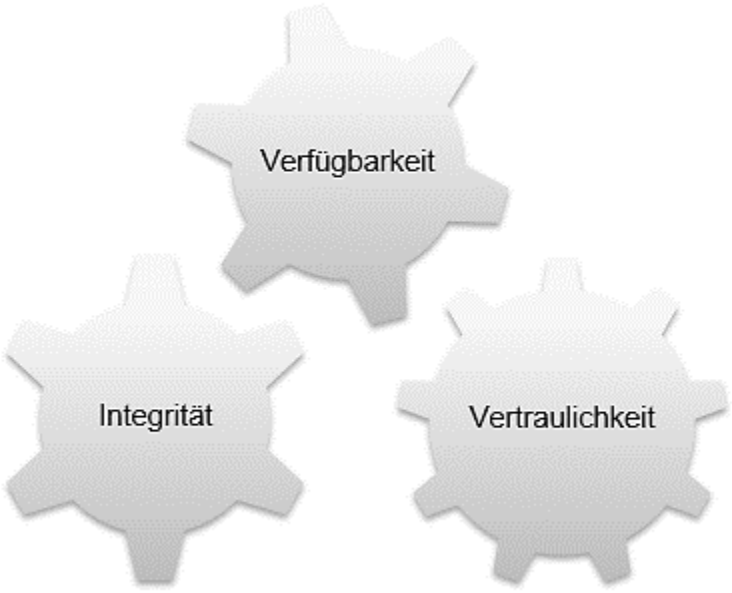


Abbildung 2: IT-Schutzziele[14]

Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit stellen den Kern dar. Weitere Schutzziele lassen sich in Authentizität, Verbindlichkeit, Zurechenbarkeit und Anonymität unterteilen.[15]

In den nachfolgenden Kapiteln werden die einzelnen Schutzziele näher erläutert. Auch auf die erweiterten Schutzziele soll näher eingegangen werden. Diese werden in der Literatur differenziert dargestellt. Die im Rahmen dieser Arbeit vorgestellten Schutzziele

[13] Vgl. Enzyklopädie der Wirtschaftsinformatik, 2016

[14] Eigene Darstellung, Daten entnommen aus: Klipper, S.: Cyber Security, S11

[15] Vgl. Klipper, S.: Cyber Security, S12ff

weisen einen starken Bezug zu IT-Sicherheit auf, zusätzlich stehen sie in direktem Zusammenhang zu den Themen Sicherheit und E-Commerce.

2.3.1. Vertraulichkeit

Das Schutzziel der Vertraulichkeit behandelt hauptsächlich die unerlaubte Informationsgewinnung. Dies bedeutet, dass Informationen von unberechtigten Personen nicht auf- oder abgerufen werden dürfen.

> *„Informationsvertraulichkeit ist bei einem IT-System gewährleistet, wenn die darin enthaltenen Informationen nur Befugten zugänglich sind.“*[16]

Das Schutzziel der Vertraulichkeit steht zumeist in einem gewissen Spannungsverhältnis zu dem Schutzziel der Verfügbarkeit. Nicht verfügbare Daten können auch nicht abgerufen werden, was jedoch im Widerspruch zur ständigen Verfügbarkeit von Informationssystemen steht. Verletzungen dieses Schutzziels werden in der Regel auch von der Öffentlichkeit beziehungsweise von Nutzern der Informationssysteme als solche erkannt und führen unweigerlich zu einem Vertrauensbruch.[17]

2.3.2. Integrität

Das Schutzziel der Integrität steht für die Absicherung eines Informationssystems und seinen Inhalten gegenüber Manipulation. Integrität steht hier für die Unverfälschtheit beziehungsweise Echtheit von Daten und Inhalten. Eine Veränderung von Inhalten eines Systems kann zu weitreichenden Schäden innerhalb des Unternehmens führen. Vor allem im Wirtschaftssektor, als Beispiel lässt sich hier die Finanz- und Börsenbranche anführen, kann eine erfolgreiche Manipulation von Prognosedaten zum finanziellen Ruin führen. Die Nutzer selbst unterschätzen in der Regel die Gefahren, welche von diesem Schutzziel ausgehen.[18]

---

[16] Ackermann T./Bedner M.: Schutzziele der IT-Sicherheit, in: Datenschutz und Datensicherheit 2010, Ausgabe 5, S323

[17] Vgl. Klipper, S.: Cyber Security, S12

[18] Vgl. Klipper, S.: Cyber Security, S12f

2.3.3. Verfügbarkeit

Mittels des Schutzziels der Verfügbarkeit soll gewährleistet werden, dass ein Informationssystem durch Angriffe nicht in dessen Verfügbarkeit eingeschränkt werden kann. Gängige Angriffsszenarien sind sogenannte „Denial of Service“ (DoS) Attacken (engl. für „Verweigerung des Dienstes“), beispielsweise ein wiederholter Angriff auf die Webseite eines E-Commerce Anbieters. Die Verarbeitung von neuen Kundenanfragen und die Funktionsweise der Webseite werden durch den Ansturm an Anfragen in ihrer Verfügbarkeit eingeschränkt, bis hin zum vollkommenen Zusammenbruch der Webseite beziehungsweise dessen Serverkapazitäten. Angriffe, welche auf das Schutzziel der Verfügbarkeit abzielen, sind jedoch nicht nur auf die Serverlandschaft eines Unternehmens beschränkt. Das gesamte Informationssystem, also auch der sogenannte Backend Bereich (administrative Aufgaben im Hintergrund), kann ein potentielles Angriffsziel darstellen und muss entsprechend abgesichert werden.[19]

2.3.4. Weitere Schutzziele

Neben dem Kern der Informationssicherheit, also den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit, lassen sich vier weitere grundlegende Schutzziele definieren.

Authentizität

Die Authentizität umfasst die Echtheit und die Glaubwürdigkeit von Objekten, nicht beschränkt auf die Objekte in einem Informationssystem. Auch die Nutzer, beispielsweise eines E-Commerce Systems, stellen ein Objekt im Sinne der Authentizität dar. Die Überprüfung gestaltet sich daher in der Praxis als sehr schwierig. Gerade deswegen erfüllt dieses Schutzziel eine sehr verantwortungsvolle Rolle, da ein Großteil der Angriffsszenarien im E-Commerce in diesen Bereich fallen. Abschließend lässt sich feststellen, dass die Authentizität einen Bereich der Integrität einnimmt.[20]

[19] Vgl. Klipper, S.: Cyber Security, S13f

[20] Vgl. Klipper, S.: Cyber Security, S14

Verbindlichkeit

Die Verbindlichkeit, auch Nichtabstreitbarkeit genannt, beinhaltet die Herstellung einer Verbindung zu Aktionen, zum größten Teil im Nachhinein. Aktionen sollen einerseits zwischen Objekten innerhalb des Informationssystems, aber auch zwischen Nutzern und dem System zugeordnet werden können. Es gibt Verbindungen zu den Schutzzielen der Authentizität und der Integrität.

Zurechenbarkeit

Die Zurechenbarkeit erweitert das Schutzziel der Verbindlichkeit beziehungsweise Nichtabstreitbarkeit um einen entscheidenden Faktor. Der zentrale Beobachtungspunkt stellt hier der Anwendende selbst dar. Es wird versucht, Handlungen auf Personenebene festzuhalten und damit an konkrete Personen zu knüpfen. Damit kann auch im Falle eines Angriffs und der damit einhergehenden Vortäuschung einer falschen Identität, der Ursprung dieses Vorfalls leichter ausgeforscht werden.[21]

Nachdem in den vorherigen Kapiteln vor allem Begriffe der IT beziehungsweise der IT-Sicherheit definiert und näher erläutert wurden, soll das abschließende Kapitel in diesem ersten theoretischen Teil den Bereich des E-Commerce behandeln.

2.4. E-Commerce

„Electronic Commerce“ (E-Commerce) ist der Überbegriff für eine Vielzahl von möglichen Prozessen und wird oftmals im Zusammenhang mit Transaktionen zwischen Wirtschaftssubjekten angeführt. Es existierten viele verschiedene Definitionen in der Literatur, welche sich je nach Quelle stark unterscheiden.[22]

[21] Vgl. Klipper, S.: Cyber Security, S14ff

[22] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing: Ein einführendes Lehr- und Übungsbuch, Berlin Heidelberg, 2015, S3f

Da in dieser Arbeit hauptsächlich auf den Bereich des elektronischen Handels und der Interaktion des Nutzers mit ebendiesem eingegangen werden soll, wird E-Commerce zunächst nach Stallmann und Wegner wie folgt definiert:

> *„E-Commerce ist die Summe aller digitalen Anbahnungs-, Aushandlungs- und/oder Abwicklungsprozesse kommerzieller Transaktionen zwischen Wirtschaftssubjekten, die über das Internet abgewickelt werden. Der Verkauf und Kauf von Gütern und Dienstleistungen steht dabei im Fokus."*[23]

Diese Definition entspricht einer enger gefassten Definition, welche vor allem die Transaktionen zwischen Wirtschaftssubjekten – in der Regel also den Konsumierenden auf Privatebene – umfassen. Im Fokus steht hier die Handels- und Marktorientierung und damit in weiterer Folge der Kauf und Verkauf von Dienstleistungen. Im weiteren Sinne behandelt E-Commerce jedoch auch Geschäftsprozesse von Unternehmen, welche über Informationstechnologien sowie deren Vernetzung unterstützt werden. Zusätzlich existieren Abgrenzungen zu dem Fachbegriff des „Electronic Business" (E-Business), welcher in der Literatur wiederum als Übergriff des E-Commerce beschrieben wird. E-Commerce stellt also einen Teilbereich von E-Business dar.[24]

E-Business

E-Business wird in der Literatur nach Wirtz wie folgt definiert:

> *„Unter dem Begriff E-Business wird die Anbahnung sowie die teilweise respektive vollständige Unterstützung, Abwicklung und Aufrechterhaltung von Leistungsaustauschprozessen zwischen ökonomischen Partnern mittels Informationstechnologie (elektronischer Netze) verstanden."*[25]

[23] Stallmann F./Wegner U.: Internationalisierung von E-Commerce-Geschäften: Bausteine, Strategien, Umsetzung, Wiesbaden, 2015, S6

[24] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S3f

[25] Wirtz, B.: Electronic Business, Wiesbaden, 2013, S22

An dieser Definition lässt sich auch der grundlegende Unterschied zu E-Commerce erkennen, nämlich die Ausdehnung auf weitere Teilbereiche wie beispielsweise der Aufrechterhaltung von Leistungsaustauschprozessen.[26]
Während im E-Commerce die Transaktion im Mittelpunkt steht, behandelt E-Business das gesamte Umfeld der Informationsverarbeitung und Vernetzung. Dazu zählen auch weiterführende Prozesse wie der gesamte Backend Bereich eines Informationssystems. E-Commerce findet nicht nur über offene Netze statt, wie beispielsweise dem Internet, sondern kann über jedes elektronische Medium beziehungsweise Netzwerk abgewickelt werden, welches für eine Transaktion geeignet ist. Dies lässt sich anhand verschiedener Dimensionen verdeutlichen. So kann die Transaktionsebene verschiedene Medien wie beispielsweise das Internet, mobile Systeme, TV Systeme bis hin zu Telefonsystemen beinhalten. Transaktionsgüter stellen unter anderem Produkte, Dienstleistungen oder auch Informationen dar. Transaktionspartner sind in der Regel Konsumierende, Selbständige oder auch öffentliche Einrichtungen.[27]

M-Commerce

Als weiterer Teilbereich des E-Commerce bezieht sich „Mobile Commerce“ auf den mobilen Sektor. Es handelt sich hierbei also um ortsunabhängige Transaktionen mittels Einsatz von mobilen Geräten wie beispielsweise Smartphones, Tablets oder auch mobile Terminals. In der Regel unterscheidet sich eine Transaktion im M-Commerce nur wenig von einer Transaktion über einen handelsüblichen Computer. Die Zahlungsabwicklung wird ebenfalls über einen Internet Browser abgewickelt. Zusätzlich besteht die Möglichkeit, Transaktionen auch über Apps durchzuführen. Ein Notebook, obwohl es durch aktuelle Technologien wie UMTS Karten oder Datensticks auch eine gewisse Ortsunabhängigkeit aufweist, wird nicht zu diesem Bereich gezählt, da es einem stationären Desktop Computer zu sehr ähnelt.[28]

---

[26] Vgl. Aichele C./Schönberger M.: E-Business: Eine Übersicht für erfolgreiches B2B und B2C, Wiesbaden, 2016, S1f

[27] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S4f

[28] Vgl. Heinemann G.: Der neue Online-Handel: Geschäftsmodell und Kanalexzellenz im Digital Commerce, Wiesbaden, 2016, S129

Entwicklung

Unbestritten ist das Wachstum im Bereich E-Commerce, wie eine aktuelle Prognose der Statista bestätigt (vgl. Tabelle 1). Die Nutzerzahlen steigen demnach pro Jahr um einen stabilen Prozentsatz im Bereich von 5 % bis 10 % an.

Jahr	Nutzer in Millionen
2015	1.469,7
2016	1.608,8
2017	1.738,0
2018	1.885,9
2019	2.046,2
2020	2.211,8
2021	2.341,4

Tabelle 1: Prognose Anzahl der E-Commerce Nutzer weltweit 2015-2021[29]

Nach der Definition der Fachbegriffe E-Commerce sowie E-Business sollen in den folgenden Kapiteln die für diese Arbeit relevanten Teilbereiche des E-Commerce näher erläutert werden. Hierzu zählt zunächst die Einschränkung auf bestimmte Transaktionspartnerschaften. Zusätzlich wird auf die Motivation der Konsumierenden eingegangen sowie die Vor- und Nachteile des E-Commerce gegenüber dem stationären Handel beleuchtet. Abschließend sollen die wichtigsten Bezahlprozesse sowie der Einsatz von Nutzerprofilen untersucht werden.

2.4.1. Geschäftsmodelle

Es existieren verschiedene Modelle im Bereich des E-Commerce, welche sich je nach den beteiligten Personen grundlegend unterscheiden. Beobachtungsgegenstand dieser Arbeit ist ausschließlich das sogenannte „Business-to-Consumer“ Modell (B2C),

[29] Daten entnommen aus: Statista: Prognose zur Anzahl der E-Commerce-Nutzer weltweit in den Jahren 2015 bis 2021 (in Millionen), URL: https://de.statista.com/statistik/daten/studie/485005/umfrage/prognose-der-e-commerce-nutzer-weltweit (abgerufen am 14.12.2016), Statista Digital Market Outlook, 2016

welches Transaktionen zwischen Unternehmen und Konsumierenden behandelt. Weitere populäre Geschäftsbereiche umfassen unter anderem „Business-to-Business“ (B2B), also Modelle zwischen Unternehmen selbst. Aber auch „Consumer-to-Consumer“ (C2C) Transaktionen nehmen einen Teil des Marktes ein. Ein populäres Beispiel für eine solche C2C Plattform stellt das Auktionshaus Ebay dar. Selbst auf staatlicher Ebene existieren Modelle wie beispielsweise „Administration-to-Business“ (A2B) welche Vorgänge zwischen staatliche Behörden beziehungsweise Einrichtungen und Unternehmen umfasst.[30]
Wirtz definiert B2C wie folgt:

> *„Im Vergleich zu B2B beschreibt B2C den Leistungsaustausch von physischen sowie digitalen Gütern und Dienstleistungen von Unternehmen (Anbieter) und einzelnen Verbrauchern (Nachfrager). Leistungsaustauschprozesse im B2C werden vorrangig über Online-Shops realisiert, über denen der Vertrieb der Waren und Dienstleistungen realisiert wird.“*[31]

Als Beispiele für B2C lassen sich Amazon, Zalando oder auch Versandhäuser wie Universal oder Quelle anführen. Die Abwicklung findet prinzipiell direkt zwischen Unternehmen und Konsumierenden statt. Dies ermöglicht einen – in der Theorie – unkomplizierten und gewinnoptimierten Prozess für beide Seiten. In der Praxis stehen jedoch die Nutzenpotentiale beziehungsweise Vorteile dieses B2C Modells durchaus auch Nachteilen gegenüber. Zahlreiche technische Besonderheiten und Einschränkungen sowie auch psychologische Besonderheiten sind zu berücksichtigen.[32] Dies soll in den folgenden Kapiteln aufgezeigt werden.

2.4.2. Nutzenpotentiale Anbieter

Durch den Einsatz von E-Commerce entstehen viele potentielle Vorteile, welche sowohl die Anbieter- als auch die Nutzerseite betreffen. In diesem Kapitel soll zunächst auf die Vorteile aus Anbietersicht eingegangen werden.

---

[30] Vgl. Aichele C./Schönberger M.: E-Business, S5ff

[31] Wirtz, B.: Electronic Business, S24

[32] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S7

Globale Präsenz

Anbieter haben die Möglichkeit, ihr Angebot – gegebenenfalls über internationale oder auch mehrsprachige Versionen ihrer Webseite – global aufzubereiten und damit einem breiten Publikum zugänglich zu machen.

Flexibilität

Ein Online Shop bietet eine hohe Flexibilität, da Produkte und Warengruppen jederzeit erweitert, reduziert oder ausgetauscht werden können. Das Platzangebot ist – abgesehen von geringen technischen Einschränkungen – unlimitiert.

Direkte Bestellannahme

Durch den im Vergleich zum stationären Handel stark verkürzten Weg der Bestell- und Auftragsannahme ergeben sich Zeit- und Kostenvorteile. Händlerinnen und Händler können so mit höheren Margen arbeiten während gleichzeitig die Vertriebswege optimiert werden.

Gewinnung von Kundendaten

Im Rahmen einer E-Commerce Transaktion kommt es unweigerlich zu einer Übermittlung von personenbezogenen Daten. Ein anonymer Kauf wie beispielsweise im stationären Handel ist nicht möglich. Dieser Umstand führt zu einem großen Potential auf der Anbieterseite, da zunächst – sofern die Einwilligung des Gegenübers vorhanden ist – die reinen Daten für Zusendungen von weiterführenden Angeboten genutzt werden können. Des Weiteren kann der Anbieter auf Basis dieser Daten auch Statistiken und Auswertungen erstellen. Beides wirkt sich absatzfördernd aus und stellt einen entscheidenden Vorteil des E-Commerce dar. Zusätzlich besteht die Möglichkeit, durch die Anlegung eines Profils verwandte beziehungsweise ähnliche Produkte direkt auf der Webseite anzubieten.

Darüber hinaus ergeben sich weitere Vorteile aus den spezifischen Merkmalen des E-Commerce wie beispielsweise der Orts- und Zeitunabhängigkeit (keine Öffnungszeiten) oder auch der Transparenz (erleichterte Informationsbeschaffung).[33]

[33] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S18f

2.4.3. Nutzenpotentiale Konsumierende

Auf der Nutzerseite lassen sich ebenso wie auf der Anbieterseite viele positive Aspekte des E-Commerce aufzählen. Nachfolgend findet sich eine Aufzählung der relevanten Potentiale.

Anywhere/Anytime Verfügbarkeit

Durch den Einsatz von elektronischen Medien und der ständigen Vernetzung lassen sich Einkäufe jederzeit und zum größten Teil ortsunabhängig durchführen. Die Vernetzung der verschiedenen E-Commerce Plattformen ermöglicht es den Konsumierenden, auch außerhalb der Öffnungszeiten des stationären Handels einzukaufen. Das Produkt kann in bestimmten Fällen, beispielsweise wenn es sich um digitale Produkte wie Downloads oder Produktschlüssel handelt, sofort bezahlt und in weiterer Folge auch bezogen werden. Analog zum Vorteil der globalen Präsenz auf der Anbieterseite, hat auch der Konsumierende die Möglichkeit, internationale Märkte zu nutzen und damit auch Produkte zu beziehen, welche lokal nicht verfügbar oder nur schwer erhältlich sind.[34]

Zeitvorteile

Einer der wichtigsten Argumente für den Kauf im stationären Handel stellt nach wie vor die Tatsache dar, dass Produkt sofort in Händen halten zu können. Dieser Umstand ist mittlerweile kein Grund mehr, E-Commerce nicht zu nutzen. Ganz im Gegenteil, durch die Einführung von „Same Day Delivery“ (SDD) können Konsumierende auf nahezu ebenso schnelle Liefermethoden zurückgreifen und zusätzlich auch noch weitere Vorteile wie alternative Zustellorte nutzen. Beratungs- und Montagepakete runden das Angebot ab. Je nach Produktgruppe kann an einem Termin die Lieferung und gleichzeitige Montage stattfinden. Dieser Vorgang erfordert im stationären Handel zumindest zwei Termine. Die Zeitvorteile sprechen also ganz klar für die Nutzung von E-Commerce.[35]

Preisvergleichsdienste und Preisniveau

Über Suchmaschinen erhält der Nutzer die Möglichkeit, Preise effizient und einfach zu vergleichen und den Anbieter mit dem besten Angebot aus Produktpreis und Lieferkonditionen auszuwählen. Das Vorhandensein von Suchmaschinen im

[34] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S19

[35] Vgl. Heinemann G.: Der neue Online-Handel, S9

E-Commerce führt zu einer erhöhten Transparenz und ist für den Nutzer höchst lukrativ. Zahlreiche Portale führen intern bereits Datenbanken von gängigen und populären Webseiten, welche in kurzen Intervallen automatisch aktualisiert werden. Als weitere Folge daraus liegt auch das Preisniveau im Online Handel weitaus niedriger als im stationären Handel. Eine Streuung der Preise existiert jedoch dennoch.[36]

Multimedialität

E-Commerce Plattformen weisen in der Regel einen hohen Grad an Interaktivität und multimedialer Unterstützung auf. Dazu zählen neben Animationen, die zumeist die Anwendung eines Produktes vorführen, auch Videos von Konsumierenden selbst (beispielsweise im Rahmen einer Rezension). Zusätzlich wird vermehrt auch die Möglichkeit der Anpassung von Produkten an individuelle Wünsche angeboten. Das fertig angepasste Modell kann in einer Voransicht begutachtet werden.[37]

Mobile Nutzungsmöglichkeit

Mobile Plattformen haben sich zunehmend zu einem weiteren „Point of Sale“ (POS) entwickelt. Es besteht die Möglichkeit, auch unterwegs Preisvergleiche anzustellen und bei Bedarf auch direkt eine Bestellung zu tätigen. Es handelt sich also nicht nur um den potentiellen Kauf von Produkten oder Dienstleistungen, sondern auch um den Informationsgewinn aus dem gesamtem Feld des Online Handels. Soziale Netzwerke spielen hier eine große Rolle, unter anderem Facebook und Instagram. Nutzungsmöglichkeiten finden sich im Meinungsaustausch, Produktrezensionen und Produktempfehlungen bis hin zu Bewertungen von Dienstleistungen, Ärztinnen und Ärzten bis hin zu Kindergärten.[38]

Neben den bereits angeführten Vorteilen und zahlreichen Nutzenpotentialen auf Seiten der Anbieter und Konsumierenden ergeben sich auch Nachteile, welche allerdings zahlenmäßig weitaus geringer ausfallen. Im folgenden Kapitel soll dennoch auf die allgemein gültigen Nachteile des Online Handels eingegangen werden.

[36] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S19f

[37] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S19

[38] Vgl. Heinemann G.: Der neue Online-Handel, S10

2.4.4. Nachteile

Nachteile im E-Commerce finden sich vor allem auf dem Gebiet der Sicherheit und der fehlenden physischen Kontaktmöglichkeit mit dem Produkt. Ein weiterer Nachteil liegt in der veränderten Handhabung von digitalen Produkten, welche durch ihre Beschaffenheit nicht mehr uneingeschränkt verfügbar sind.

Fehlende physische Kontakte

Selbst unter Verwendung von aufwendigen Produktvideos und Animationen, einen Ersatz für das direkte Besichtigen und Hand anlegen gibt es nicht. Der Konsumierende kann ein Produkt weder berühren, noch kann er es fühlen, schmecken oder riechen. Dadurch sinkt in der Regel die Kaufbereitschaft, da der Mensch intuitiv über seine Sinne gesteuert wird. Es bleiben also mitunter impulsiv motivierte Käufe aus, zusätzlich leidet auch die Entscheidungsfähigkeit darunter.

Digitale Güter

Der Einsatz von digitalen Produkten stellt auf beiden Seiten potentielle Risiken dar. So befürchtet der Anbieter illegale Verbreitung und Vervielfältigung, während der Nutzer in seinen Möglichkeiten der Weitergabe – mitunter auch dem Weiterverkauf – beeinträchtigt wird. Einige digitale Güter setzen auch eine aktive Internetverbindung voraus. Dieser Umstand kann im Falle eines Netzwerkausfalles dazu führen, dass eigene Produkt nicht mehr verwenden zu können.[39]

Bezahlmöglichkeiten

Der Vorgang der Bezahlung im E-Commerce entspricht einem komplexen Prozess, da der Einsatz und die Durchführung von „E-Payments“, also von elektronische Zahlungen, eine Vielzahl von Anforderungen erfüllen muss (vgl. Kapitel 2.5.1.). Sollte es zu Problemen während der Verarbeitung kommen, ist oftmals eine manuelle Korrektur notwendig. Dies verursacht zusätzliche Aufwände auf der Anbieter- und Nutzerseite.[40]

Die grundlegenden Anforderungen an E-Payments sowie die vielen verschiedenen Möglichkeiten der Zahlungsabwicklung werden im folgenden Kapitel näher betrachtet.

---

[39] Vgl. Olbrich R./ Schultz C. D./Holsing C.: Electronic Commerce und Online-Marketing, S23

[40] Vgl. Aichele C./Schönberger M.: E-Business, S43f

2.5. Zahlungsabwicklung

Bezahlmöglichkeiten im E-Commerce setzen sich zunächst aus dem stationären Handel bekannten herkömmlichen Methoden zusammen. Des Weiteren werden moderne Zahlungsmöglichkeiten eingesetzt, welche sich die Vernetzung der Kommunikations- beziehungsweise Transaktionsbeteiligten zunutze machen. Je nach Zahlungsmittel kann ein unterschiedlicher Grad an Sicherheit beobachtet werden. Die Auswahl der angebotenen Bezahldienste wird vom Anbieter festgelegt, der Konsumierende kann aus den vorhandenen Diensten seine bevorzugte Zahlungsart auswählen.[41]

2.5.1. Anforderungen

Während es an die klassischen Zahlungsanforderungen wie beispielsweise Vorkasse oder Rechnung keine speziellen Anforderungen gibt, müssen E-Payments eine Reihe von Kriterien erfüllen.

Totalität

Eine Transaktion soll in ihrem vollen Umfang durchgeführt werden. Sollte dies nicht möglich sein, muss der vorhergehende Zustand wiederhergestellt werden.

Konsistenz

Die Transaktionsbeteiligten müssen sich über den Inhalt eines Auftrages einig sein. Sämtliche relevante Informationen wie die Höhe des Gesamtbetrages, der Grund beziehungsweise der Gegenstand der Zahlung sowie auch die persönlichen Daten der Personen müssen übereinstimmen und klar ersichtlich sein.

Unabhängigkeit

Mehrfach ausgeführten Bestellungen des mitunter identischen Produktes muss gegengesteuert werden. Es darf nicht möglich sein, ein einzelnes Exemplar mehrfach zu vergeben beziehungsweise dieses zu bezahlen.[42]

[41] Vgl. Aichele C./Schönberger M.: E-Business, S43ff

[42] Vgl. Aichele C./Schönberger M.: E-Business, S44

Dauerhaftigkeit

Durch unter anderem technisch bedingte Ausfälle des Systems sollen keine Transaktionsdetails verloren gehen. Erfolgreich durchgeführte Zahlungen müssen unmittelbar gesichert und an sicherer Stelle als Backup abgelegt werden. Nur so kann der vorherige Zustand wiederhergestellt werden.

Die grundlegenden Anforderungen an E-Payments werden durch zusätzliche Faktoren wie Verlässlichkeit, Fälschungssicherheit, Internationalität oder Konvertierbarkeit ergänzt. Verschiedene Kriterien helfen, die verfügbaren E-Payment Lösungen zu klassifizieren. Zu diesen zählt unter anderen die regionale Verbreitung, das jeweilige Anwendungsszenario, die Höhe des Transaktionsbetrages bis hin zu dem technologischen Konzept, der Anonymität und dem Zeitpunkt der Zahlung.[43]
In den folgenden Kapiteln sollen die wichtigsten Zahlungsarten vorgestellt, und auch kategorisiert werden.

2.5.2. Klassische Zahlungsverfahren

Zu den klassischen Zahlungsverfahren zählen die Zahlung auf Rechnung, die Vorkasse, die Lastschrift und die Zahlung per Nachnahme.[44]
Im Rahmen dieser Arbeit wird eine Auswahl aus diesen Verfahren betrachtet, welche im Bereich des B2C besondere Verwendung finden.

Zahlungsabwicklung per Vorkasse

Die Bezahlung per Vorkasse erfolgt vor der Lieferung der Ware beziehungsweise der Erbringung einer Dienstleistung. Diese Methode stellt für den Anbieter nur ein sehr niedriges Risiko dar, da er vor einem möglichen Zahlungsausfall oder einem Zahlungsverzug geschützt wird. Dafür entstehen dem Anbieter einige administrative Aufwände, da er die Zahlung vor der weiteren Bestellabwicklung zuordnen muss. Dies kann zwar je nach System auch automatisiert passieren, dennoch sind hierfür eigene Prozesse notwendig um auch mögliche Stornierungen und Rückbuchungen durchführen zu können.[45]

---

[43] Vgl. Aichele C./Schönberger M.: E-Business, S44f

[44] Vgl. Heinemann G.: Der neue Online-Handel, S99

[45] Vgl. Aichele C./Schönberger M.: E-Business, S45f

Der Konsumierende trägt bei dieser Zahlungsart das Risiko von Lieferverzögerungen und einer verzögerten Rückbuchung bei Stornierungen oder Reklamationen. Zusätzlich kommt es auch – ähnlich wie auf der Anbieterseite – zu einem administrativen Mehraufwand, da die Zahlungsdaten zumeist manuell in die Formulare des Online Banking Anbieters übertragen werden müssen. Als Vorteil lässt sich die hohe Sicherheit anführen, da keine unmittelbaren Zahlungsdaten über die Webseite des Anbieters laufen. Wie die Zahlung letztendlich durchgeführt wird, bleibt offen. Dem Nutzer stehen neben der Einzahlung des Betrages über die niedergelassene Bankfiliale bis hin zu der Verwendung von Online Banking auch moderne Formen der Überweisung wie Giropay oder Sofortüberweisung zur Verfügung. Diese ermöglichen eine unkomplizierte Bezahlung über die Online Banking Plattform mittels Verwendung einer Transaktionsnummer (TAN).[46]

Zahlungsabwicklung per Lastschrift

Die Zahlung per Lastschrift stellt eine einfache und unkomplizierte Variante dar. Neben dem initialen Aufwand der Übermittlung der Kontodaten, welches nur ein sehr geringes Risiko für den Konsumierenden darstellt, wird die zukünftige Zahlungsabwicklung vollkommen automatisch abgewickelt. Das Risiko liegt hier beim Anbieter, da zumeist ohne ein entsprechendes Mandat beziehungsweise eine schriftliche Einverständniserklärung des Nutzers gearbeitet wird. Dieser hat bei unrechtmäßigem Einzug die Möglichkeit, die Beträge innerhalb von acht Wochen zurückzufordern, ohne Angabe von weiteren Gründen.[47]

Neben den klassischen Zahlungsverfahren soll im folgenden Kapitel auf die Zahlung mittels Kreditkarte näher eingegangen werden.

2.5.3. Kreditkarten

Die Zahlung per Kreditkarte ist ein weltweit anerkanntes und gängiges Verfahren, welches sich auf viele verschiedene Anbieter aufteilt. Dazu zählen neben Visa, MasterCard und American Express noch viele weitere Kreditkartenfirmen.

---

[46] Vgl. Aichele C./Schönberger M.: E-Business, S45f

[47] Vgl. Aichele C./Schönberger M.: E-Business, S46f

Der Bezahlvorgang startet mit der Eingabe der Kreditkartennummer im Portal des E-Commerce Anbieters. Im Hintergrund sind hier mehrere Parteien involviert, von dem der Konsumierende jedoch nichts bemerkt. Die Daten werden an einen sogenannten „Payment Service Provider“ (PSP) weitergeleitet, welcher diverse Sicherheitsüberprüfungen durchführt. Dies geschieht in Echtzeit und vollständig automatisiert. Nachdem dieser Schritt erfolgreich durchgeführt wurde, kann die Transaktion seitens des Anbieters freigegeben werden. Die Transaktionsdaten werden in der Zwischenzeit auch an die Bank des Konsumierenden sowie an die Bank des Anbieters weitergeleitet. Auf Anbieterseite fallen für diesen Vorgang, vor allem durch die Inanspruchnahme des Payment Service Providers, zusätzliche Gebühren an. Außerdem stellt die Integration der Prozesse einen erheblichen Mehraufwand dar. Als Vorteil lässt sich die Transaktionsabwicklung selbst anführen, welche einem sicheren und etablierten Prozess entspricht. Auch die Möglichkeit von internationale Zahlungen lässt sich mit der Kreditkarte stark vereinfachen.[48]

2.5.4. E-Payments

Die Gruppe der elektronischen Zahlung unterliegt einer stetigen Entwicklung und Veränderung. Neben populären und bekannten Anbietern wie PayPal oder Sofortüberweisung etablieren sich auch alternative Zahlungsmethoden wie die Verwendung von Guthabenkarten oder die Plattform ClickandBuy.[49]
Die verschiedenen E-Payment Methoden wurden speziell für den Bereich des E-Commerce entwickelt und lassen sich grundlegend in drei Kategorien einteilen.

Nutzerkontoabhängige Verfahren

Diese Verfahren setzen ein Nutzerkonto sowie eine entsprechende Registrierung und Freischaltung voraus. Je nach Anbieter wird ein unterschiedlicher Detailgrad an persönlichen Informationen beziehungsweise Stammdaten verlangt. Der Umfang reicht von Name und E-Mail Adresse bis hin zu Adresse, Telefonnummer, Geburtsdatum, Kontoverbindung oder auch einer behördlichen Legitimation.

[48] Vgl. Aichele C./Schönberger M.: E-Business, S48f

[49] Vgl. Heinemann G.: Der neue Online-Handel, S99

Nutzerkontounabhängige Verfahren

Diese Verfahren setzen den Erwerb einer Guthabenkarte voraus, welche im stationären Handel oder auch Online erhältlich sind. Ein Nutzerkonto oder eine namentliche Registrierung wird nicht vorausgesetzt. Die Zahlungsabwicklung wird in der Regel über die Eingabe eines Codes initiiert, welcher auf Seiten des Anbieters überprüft und freigegeben wird. Karten können entweder neu gekauft, oder auch aufgeladen werden.[50]

Direktüberweisungsverfahren

Im Rahmen dieser Zahlungsmethode wird das Online Banking Portal des Konsumierenden verwendet. Populäre Anbieter wie beispielsweise Giropay oder Sofortüberweisung stellen als E-Payment Anbieter die Verbindung zwischen der Anbieterseite und der Hausbank des Nutzers her.[51]

Unterschiede bestehen im Ablauf der Transaktion. Während Giropay den Konsumierenden direkt auf das jeweilige Online Portal seiner Bank weiterleitet, es kommt also zu keiner Zwischenspeicherung auf Seiten von Giropay, findet die Kommunikation bei Sofortüberweisung zunächst zwischen Nutzer und dem E-Payment Anbieter statt. Da es sich in jedem Fall um eine Art der Vorkasse handelt, nimmt das Vertrauen in die eingesetzte Methode eine entscheidende Rolle ein.[52]

Die Zahlungsabwicklung wird zunächst durch die Auswahl der E-Payment Variante gestartet. Die Transaktion selbst findet auf der Bezahlseite des E-Payment Providers statt, welche auch in das Online Portal des Anbieters integriert werden kann. Nach erfolgreicher Zahlung und der Bestätigung des Providers kann die Bestellung getätigt werden. Der Anbieter erhält in der Regel eine Zahlungsgarantie, muss jedoch auch Gebühren an den E-Payment Provider abgeben. Da es durch den offenen und stetig wachsenden Markt zwar zu einer steigenden Nachfrage an E-Payment Lösungen kommt, gleichzeitig aber die Konsumierenden unbekannten Zahlungsarten skeptisch gegenüberstehen, konnten sich nur wenige E-Payment Provider am Markt durchsetzen. Beispiele hierfür sind unter anderem PayPal oder auch ClickandBuy.[53]

---

[50] Vgl. Stahl E./Wittmann G./Krabichler T./Breitschaft M.: E-Commerce-Leitfaden, Regensburg, 2012, 4-15

[51] Vgl. Stahl E./Wittmann G./Krabichler T./Breitschaft M.: E-Commerce-Leitfaden, 4-16

[52] Vgl. Stahl E./Wittmann G./Krabichler T./Breitschaft M.: E-Commerce-Leitfaden, 4-17f

[53] Vgl. Aichele C./Schönberger M.: E-Business, S49f

3. Risiken im E-Commerce

Nachdem im ersten Teil dieser Arbeit die wichtigsten Begriffe und Zusammenhänge erläutert wurden, soll in diesem Kapitel zunächst auf die Risikowahrnehmung des Nutzers eingegangen werden. In weiterer Folge sollen die zahlreichen konkreten Risiken im E-Commerce aufgezählt, und ihre Gegenmaßnahmen beleuchtet werden. Diese umfassen sowohl Themen der IT-Sicherheit, aber auch den Schutz der Privatsphäre und die Berücksichtigung von Sicherheitsstandards und Gütesiegel. Dieser Teil stellt die Grundlage für den empirischen Teil (vgl. Kapitel 4.) dieser Arbeit dar.
Da der Fokus dieser Arbeit nicht auf M-Commerce, sondern E-Commerce im Allgemeinen liegt, kommt es zu keiner Unterscheidung zwischen diesen beiden Kanälen. Ein elektronisch abgewickelter Bestellvorgang kann sowohl auf mobilen Geräten, als auch über einen handelsüblichen Desktop Computer oder ein Notebook erfolgen. Vielmehr liegt der Fokus auf den Web Applikationen selbst, welche über einen Browser aufgerufen werden können.

3.1. Risikowahrnehmung

Die Risikowahrnehmung wird von vielen verschiedenen Einflussgrößen getragen, welche je nach Typ und Ausprägung unterschiedlich stark ausfallen. Die Summe aller Einflussgrößen, welche sich zusätzlich gegenseitig beeinflussen, resultiert in einer individuellen Risikowahrnehmung. Es gilt also zunächst abzuklären, welche personenbezogenen Einflussgrößen vorhanden sind. Neben den personenbezogenen wird in produkt- und situationsbezogene Einflussgrößen unterteilt. Daraus ergibt sich das wahrgenommene Risiko, welches wiederum in funktionale, finanzielle, persönliche und zeitliche Risiken aufgeteilt werden kann.[54]

[54] Vgl. Heinemann G.: Der neue Online-Handel, S227ff

Die Summe aus diesen Faktoren ergibt die Bereitschaft, über einen bestimmten E-Commerce Kanal einzukaufen (vgl. Abbildung 3).[55]

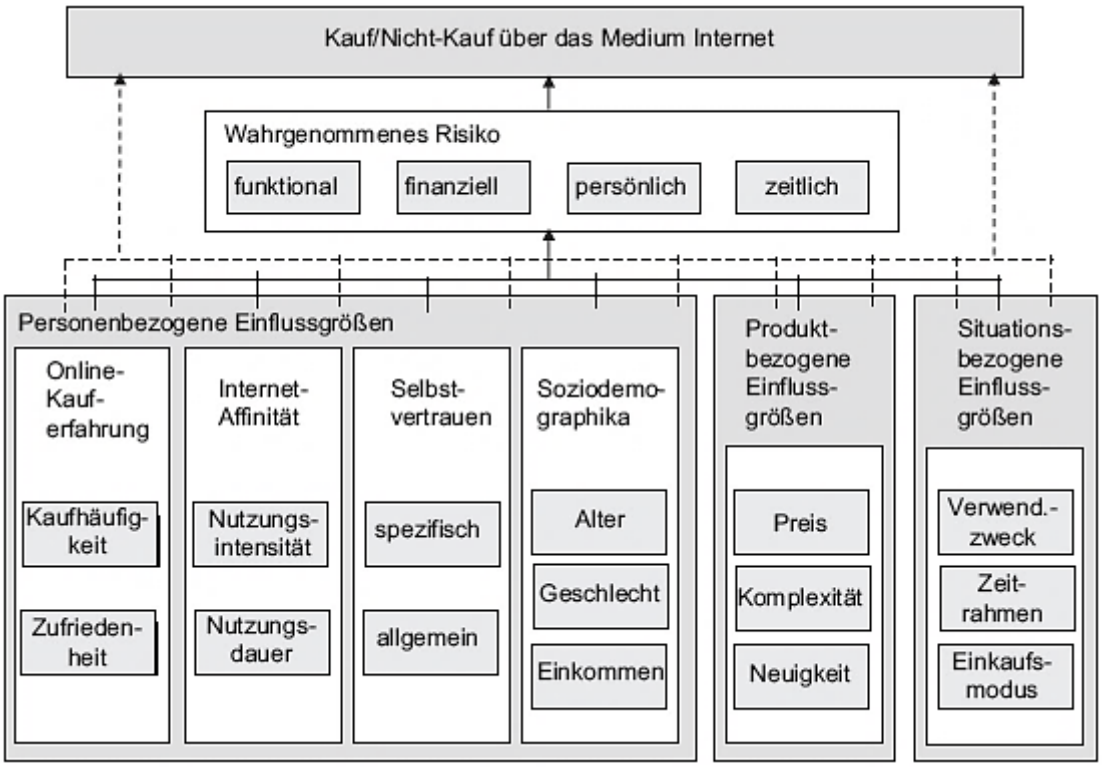


Abbildung 3: Einflussgrößen auf die Risikowahrnehmung[56]

Personenbezogene Einflussgrößen stellen die soziodemographischen Merkmale dar. Dazu zählt das Alter, das Geschlecht und das Einkommen des Nutzers. Des Weiteren wird in die Online-Kauferfahrung, die allgemeine Internet-Affinität und das Selbstvertrauen unterteilt. Die Erfahrung in Verbindung mit E-Commerce wird durch die Häufigkeit der Nutzung sowie die Zufriedenheit angegeben. Durch die Nutzungsintensität und -dauer ergibt sich eine allgemeine Internet-Affinität. Auch das Selbstvertrauen spielt eine Rolle in diesem Zusammenhang, auch bei unerfahrenen Konsumierenden. Zu den produktbezogenen Einflussgrößen zählen neben dem Preis auch der Grad der Komplexität sowie der Neuigkeitswert des Produktes.[57]

[55] Vgl. Heinemann G.: Der neue Online-Handel, S227ff

[56] Abbildung entnommen aus: Heinemann G.: Der neue Online-Handel, S228

[57] Vgl. Heinemann G.: Der neue Online-Handel, S228

Der Verwendungszweck zählt zu der Gruppe der situationsbezogenen Einflussgrößen. Der zeitliche Rahmen – beispielsweise Zeitdruck – und der Einkaufsmodus ergänzen diese Kategorie. Nachfolgend sollen die verschiedenen Arten der Risikowahrnehmung erläutert werden.

Funktionales Risiko

Bedenken bezüglich der Funktionalität eines Produktes sind üblicher Bestandteil des E-Commerce. Wie bereits in Kapitel 2.4.4. angeführt, führt der fehlende physische Kontakt mit dem Produkt zu einer erhöhten Risikowahrnehmung beziehungsweise zu Zweifel seitens des Konsumierenden. Der Anbieter kann hier entweder durch ein Angebot von bekannten Marken (Markenware), ein allgemein gültiges oder erweitertes Umtauschrecht oder durch seine eigene Reputation entgegenwirken.

Finanzielles Risiko

Das finanzielle Risiko umfasst zunächst das Risiko während des Bezahlvorgangs. Zusätzlich stellt auch der Versand sowie ein möglicher Rückversand ein mögliches Risiko dar. Je nach Bezahlsystem wird vom Nutzer ein unterschiedlicher Grad an Vertrauen entgegengebracht. Das Angebot von unterschiedlichen Zahlungsmethoden, darunter auch gänzlich sichere Systeme wie die Zahlung per Vorkasse (vgl. Kapitel 2.5.2.) können die Risikowahrnehmung senken. Ein Restrisiko verbleibt aber selbst bei der Zahlung per Vorkasse beim Konsumierenden. Lieferverzögerungen bis hin zum gänzlich ausbleibenden Versand der Ware sind mögliche Szenarien. Auch beim Versand beziehungsweise Rückversand kann das Risiko, je nach Lieferkonditionen und den allgemeinen Geschäftsbedingungen, zur Gänze oder auch teilweise beim Nutzer liegen.

Persönliches Risiko

Die Themen Datenschutz und persönliche Daten stellen den Kern dieser Kategorie dar. Je nach Plattform wird ein unterschiedlicher Grad an Informationen benötigt, dessen Ausprägung direkt zu der individuellen Risikowahrnehmung beiträgt. Besonders ausschlaggebend stellen vertrauliche Daten wie beispielsweise Adressdaten, die Telefonnummer oder die Angabe der Bankverbindung dar.[58]

[58] Vgl. Heinemann G.: Der neue Online-Handel, S228

Zeitliches Risiko

Unabhängig von der Zahlungsart kann es durch Lieferverzögerungen oder sonstigen Lieferschwierigkeiten (beispielsweise kann das Produkt am Versandweg verloren gehen) zu einem langwierigen Versandprozess und damit zu einer mitunter erheblichen Verzögerung kommen. Der Reklamationsablauf ist mitunter ebenfalls mit einem mittleren bis hohen Zeitaufwand behaftet, je nachdem welche Kommunikationskanäle seitens des Anbieters verwendet werden (beispielsweise E-Mail, Telefon oder auch Online Formulare). Daher führt auch die Rückgabe beziehungsweise der Umtausch zu einem erhöhten Risiko. Selbst der persönliche Aufwand durch Bewältigung der Strecke zu der nächsten Post- beziehungsweise Speditionsfiliale zählt zu dieser Kategorie.[59]

Die Risikowahrnehmung des Nutzers lässt sich zunächst vor allem aus dem individuellen finanziellen Risiko ableiten. Großen Einfluss auf die Wahrnehmung haben auch die Einflussgrößen Kaufhäufigkeit, Zufriedenheit und das individuelle Selbstvertrauen.[60]
In den nachfolgenden Kapiteln soll daher auf die von dem Nutzer wahrnehmbaren Sicherheitsmerkmale sowie deren mögliche Gegenmaßnahmen eingegangen werden. Die Möglichkeit, den Level an Sicherheit einer E-Commerce Plattform beziehungsweise eines E-Commerce Vorgangs einzuschätzen, stellt eine wichtige Eigenschaft in Verbindung mit Transaktionen im E-Commerce dar.

3.2. Authentifizierung

Die erfolgreiche Authentifizierung stellt einen der wichtigsten Vorgänge während einer E-Commerce Transaktion dar. Dieses Risiko steht in unmittelbarem Zusammenhang zu den zahlreichen Schutzzielen der IT-Sicherheit (vgl. Kapitel 2.3.). Sollte eine E-Commerce Plattform nur unzureichende Möglichkeiten der Nutzerauthentifizierung bieten, führt dies zu einer breiten Angriffsfläche und einer möglichen Kompromittierung von Daten. Die Authentifizierung beinhaltet eine Vielzahl von Komponenten, auf welche in den nachfolgenden Kapiteln näher eingegangen werden soll.[61]

---

[59] Vgl. Heinemann G.: Der neue Online-Handel, S228

[60] Vgl. Heinemann G.: Der neue Online-Handel, S229

[61] Vgl. Lepofsky R.: The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web, New York, 2012, S22

3.2.1. Passwort

Die Verwendung von schwachen Passwörtern, oder auch die Verwendung von identischen Passwörtern für eine Vielzahl von Plattformen, stellt ein hohes Sicherheitsrisiko dar. Des Weiteren sollen Passwörter auch regelmäßig geändert werden, um das Zeitfenster für mögliche Angriffe auf das Passwort klein zu halten. Sollte das Passwort erfolgreich erraten werden, kann der Angriff zunächst die persönlichen Daten des Nutzers kompromittieren und in weiterer Folge auch finanziellen Schaden anrichten (beispielsweise durch das Tätigen von Bestellungen).
Als Gegenmaßnahme lässt sich die Verwendung von starken und damit auch sicheren Passwörtern anführen. Aber auch Maßnahmen wie die Steuerung der Gültigkeitsdauer der Passwörter und ergänzende Kriterien wie die Prüfung auf Gleichheit zu vorherigen Passwörtern stellen wirkungsvolle Sicherheitsmaßnahmen dar.[62]

Passwortstärke

Es gibt zwei verschiedene Möglichkeiten, Passwortsicherheit zu erlangen. Zum einen kann seitens des Anbieters eine bestimmte Passwortstärke vorgegeben werden, zum anderen kann auch der Nutzer selbst ein entsprechend starkes Passwort vergeben. In jedem Fall sollte das Passwort gewisse Kriterien erfüllen. Neben einer Mindestanzahl an Zeichen sollten auch Sonderzeichen, Klein- und Großbuchstaben sowie numerische Werte verwendet werden. In der Literatur wird ein Basisschutz von mindestens acht Zeichen in Verbindung mit zumindest einem numerischen Wert, einem Sonderzeichen und der Verwendung von Groß- als auch Kleinbuchstaben angegeben. Eine Erhöhung dieser Kriterien kann dazu führen, dass Passwörter vermehrt aufgeschrieben werden und der gewünschte Effekt damit nicht mehr erzielt werden kann.[63]

Ablauf und Gültigkeitsdauer

Die Steuerung der Lebensdauer von Passwörtern stellt eine effektive Sicherheitsmaßnahme dar. Zusätzlich sollte sich das neu gesetzte Passwort von dem

[62] Vgl. Lepofsky R.: The Manager's Guide to Web Application Security, S22f

[63] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis: Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse, Wiesbaden, 2015, S204f

zuletzt verwendeten, im Idealfall sogar zu sämtlichen innerhalb eines festgesetzten Zeitraums verwendeten Passwörtern, unterscheiden.[64]

Sperre

Nach einer festgelegten Anzahl von erfolglosen Anmeldeversuchen soll der Zugang für eine gewisse Zeit gesperrt werden. Zusätzliche Sicherheit bietet die Information an den Nutzer über die erfolglosen Anmeldeversuche, beispielsweise per E-Mail oder SMS. Dadurch kann einem potentiellen Angriff frühzeitig entgegengewirkt werden.[65]

Das Thema Passwortsicherheit kann durch weitere Sicherheitsmaßnahmen ergänzt werden. Einen hohen Risikofaktor weist speziell die Art der Authentifizierung sowie die Verwendung unsicherer Kanäle auf.

3.2.2. Authentifizierungsmethoden

Die einfachste Form der Authentifizierung entspricht der sogenannten 1-Faktor-Authentifizierung. Zusätzliche Sicherheit bietet die 2-Faktor-Authentifizierung beziehungsweise in besonders schützenswerten Bereichen auch die 3-Faktor-Authentifizierung. Die möglichen Faktoren lassen sich Tabelle 2 entnehmen.

Faktor	Beispiel
Wissen	Passwort
Besitz	Hardware Token, Zertifikat
Merkmal	Biometrie

Tabelle 2: Mögliche Faktoren von Authentifizierungsmethoden[66]

Werden zumindest zwei verschiedene Faktoren eingesetzt, spricht man auch von einer Mehrfaktor-Authentifizierung.

[64] Vgl. Lepofsky R.: The Manager's Guide to Web Application Security, S49

[65] Vgl. Lepofsky R.: The Manager's Guide to Web Application Security, S48

[66] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S191

Im Bereich des E-Commerce wird hauptsächlich die 1-Faktor-Authentifizierung eingesetzt (Wissen), alternativ auch die Kombination aus dem Passwort und einem Hardware Token. Dieser Token wird für die Generierung eines sogenannten Einmalpasswortes verwendet, als Medium dienst zumeist das Mobiltelefon durch Versand des Codes per SMS (vgl. Abbildung 4).[67]

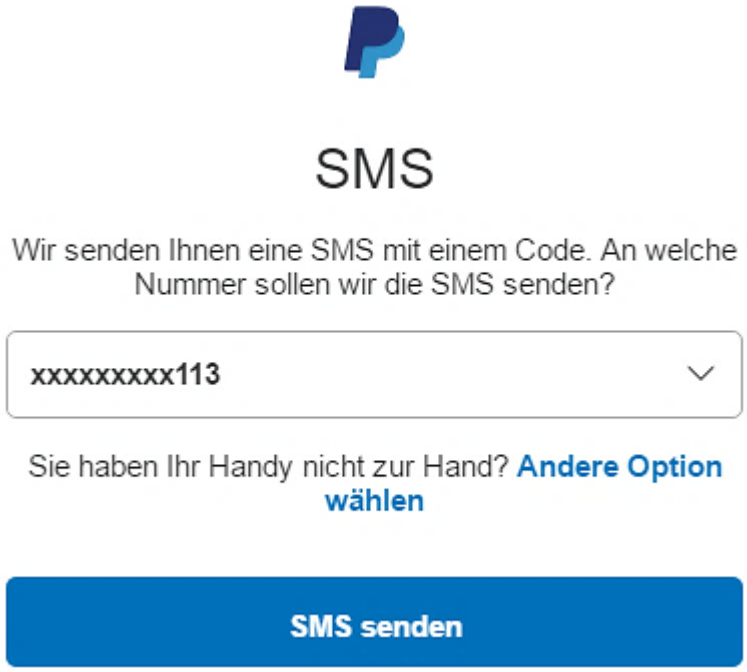


Abbildung 4: 2-Faktor-Authentifizierung bei PayPal[68]

Weitere Möglichkeiten bieten separate Hardware Token oder auch statische Listen, welche per Post versendet werden. Hardware Token können wiederum in „Soft Token“ und „Hard Token“ unterschieden werden. Erstere können als Applikation auf einem Fremdgerät installiert werden (Smartphone, Tablet), letztere weisen einen höheren Grad an Sicherheit auf.[69]

[67] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S191f

[68] Eigene Darstellung, Screenshot aus: Google Chrome, Version 55.0.2883.87, URL: https://www.paypal.com

[69] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S191f

3.2.3. Verschlüsselung

Die Übertragung der Passwörter sollte stets verschlüsselt erfolgen. Eine unverschlüsselte Übertragung stellt ein hohes Sicherheitsrisiko dar, da potentielle Angreiferinnen und Angreifer das Passwort im Klartext abfangen und weiterverwenden können. Für die Übertragung der Passwörter hat sich netzwerkseitig die Verwendung des HTTPS Protokolls etabliert. HTTPS steht für „Hypertext Transfer Protocol“ beziehungsweise „HTTP over SSL“, also der Erweiterung des handelsüblichen HTTP Protokolls um SSL (Secure Socket Layer). Die aktuellen Versionen des SSL Protokolls wurden mittlerweile in TLS (Transport Socket Layer) umbenannt, daher spricht man auch von „HTTP over TLS“. Wie in Abbildung 5 ersichtlich, ist für den Nutzer die Verwendung des HTTPS Protokolls direkt in der Adresszeile des Browsers ablesbar.[70]

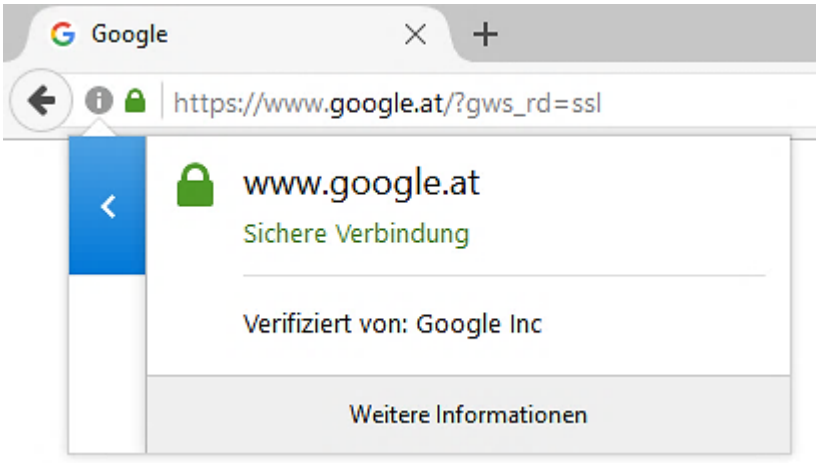


Abbildung 5: Verwendung von HTTPS[71]

Die Verwendung von HTTPS macht es potentiellen Angreiferinnen und Angreifern unmöglich, Passwörter im Klartext auszulesen. Des Weiteren dient es der erfolgreichen Authentifizierung zwischen zwei Endpunkten. Es kann eine Punkt-zu-Punkt Verschlüsselung erreicht werden, und zwar von dem verwendeten Browser ausgehend (beispielsweise Microsoft Internet Explorer, Google Chrome oder auch Mozilla Firefox) bis hin zu dem Ort, an dem die Verbindung endet. In den meisten Fällen entspricht dies

[70] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S151f

[71] Eigene Darstellung, Screenshot aus: Mozilla Firefox, Version 50.1.0, URL: https://www.google.at

dem Webserver des E-Commerce Anbieters. Besondere Bedeutung kommt der Version des eingesetzten Algorithmus zu, da immer wieder Sicherheitslücken aufgedeckt werden. Empfohlen wird daher der Einsatz der TLS Version 1.2 oder höher.[72]

3.3. Session Management

Mittels eines Session Managements wird der gesamte E-Commerce Vorgang zwischen Anbieter und Nutzer verwaltet beziehungsweise abgewickelt. Hierzu zählt die Authentifizierung selbst, die Interaktionen mit der Webseite (beispielsweise der Warenkorb) und letztendlich auch die Bestellung und Zahlungsabwicklung. Hierzu wird zunächst eine Session ID, also eine vom Webserver generierte zufällige Nummer generiert und an den Browser des Nutzers gesendet. Die Konfiguration dieser Session ID und die daraus folgende Kommunikation kann zu einem großen Sicherheitsrisiko führen da es bei Verwendung von unzureichenden Sicherheitsmaßnahmen zu einer Übernahme der Session kommen kann (dem sogenannten „Session Hijacking“).[73]
Nachfolgend sollen meistverbreitete Risiken angeführt werden sowie auf deren Gegenmaßnahmen eingegangen werden.

3.3.1. Zufälligkeit der Session ID

Damit es für den Angreifer möglichst schwierig ist, die Session ID ohne zusätzliche Hilfsmittel (beispielsweise Schadsoftware auf dem Zielsystem) zu erraten, sollte diese möglichst komplex und zufällig generiert werden. Das Risiko der Übernahme der Session verschärft sich, wenn sich der Nutzer bereits authentifiziert hat. In diesem Fall können nicht nur Informationen wie der Warenkorbinhalt, sondern unter Umständen auch die vollständigen Anmelde- und Stammdaten eingesehen werden. Der Nutzer kann die Session ID entweder direkt in der Adresszeile des Browsers erkennen, oder sie über die gespeicherten Cookies (vgl. Kapitel 3.4.) einsehen. Das Setzen der Session ID über Cookies stellt eine sichere und moderne Variante dar, da der in der Adresszeile des Browsers angezeigte URL auch in einer Vielzahl von Logs auf Server- und Clientebene gespeichert wird. Die grundsätzliche Deaktivierung von Cookies ist nicht

[72] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S294ff

[73] Vgl. Lepofsky R.: The Manager’s Guide to Web Application Security, S23ff

empfehlenswert, da in diesem Fall automatisch auf die Vergabe der Session ID innerhalb der URL umgeschaltet wird, woraus sich ein deutlich höheres Sicherheitsrisiko ergibt. Browser bieten zur Überprüfung der Session ID eingebaute Funktionen an, darüber hinaus werden auch Erweiterungen (Plugins) angeboten, welche Informationen wie die Session ID und weitere Verbindungsdetails anzeigen. Die Verwendung und Überprüfung der Session Daten ist empfehlenswert und trägt deutlich zur Sicherheit einer E-Commerce Plattform bei.[74]

Abbildung 6 zeigt die gesetzte Session ID im Falle des Online Händlers Amazon.

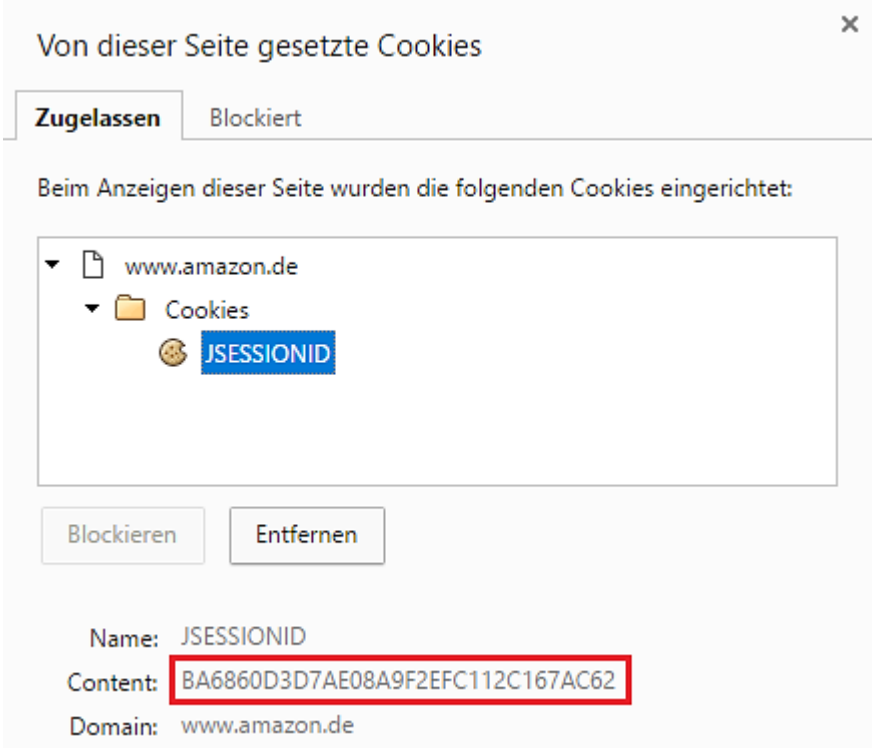


Abbildung 6: Abruf und Überprüfung der Session ID[75]

[74] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S213ff

[75] Eigene Darstellung, Screenshot aus: Google Chrome, Version 55.0.2883.87, URL: https://www.amazon.de

Mittels dieses Dialogfensters lässt sich sowohl die Session ID einsehen, als auch überprüfen ob und wann diese abläuft beziehungsweise vom System entfernt wird. Zusätzlich kann der Nutzer spezifische Cookies manuell löschen (direkt über die Schaltfläche im Dialogfenster).[76]

3.3.2. Persistente Sessions

Persistente Sessions beinhalten die Speicherung beziehungsweise Aufrechterhaltung der Session selbst nach Beendigung des Browsers oder dem Ausschalten des Gerätes. E-Commerce Plattformen bieten dem Nutzer mitunter verschiedene Optionen an, woraus direkt zwischen einer persistenten oder temporären Session ID gewählt werden kann. Zumeist geschieht dies während des Anmeldevorgangs mittels einer speziellen Auswahl, ob der Nutzer dauerhaft angemeldet bleiben möchte.

Da das Design einer Session prinzipiell den Erhalt des Zustandes einer Webseite beinhaltet, sollte bei Verlassen der jeweiligen Plattform stets die Abmeldefunktion genutzt werden. Die dafür vorgesehenen Schaltflächen garantieren den sofortigen Verwurf der Session ID. Ansonsten verbleibt die Session ID im Speicher des Browsers beziehungsweise innerhalb der jeweiligen Cookies und kann bis zum Abmeldevorgang, der nächsten Bereinigung der Cookies oder dem Ablauf der Session weiterhin übernommen werden. Die Bereinigung der Cookies kann je nach Benutzereinstellung manuell, nach dem Schließen des Browsers oder auch in regelmäßigen zeitlichen Abständen geschehen. Die sicherste Variante stellt ein Bereinigen der Cookies nach dem Schließen des Browsers dar. Moderne Browser wie Google Chrome bieten zusätzlich an, nur spezifische Cookies beim Beenden zu löschen während unbedenkliche Cookies erhalten bleiben können.[77]

3.3.3. Session Timeout

Die Zeitspanne, nachdem ein Nutzer vom System automatisch abgemeldet wird, stellt ein wichtiges Sicherheitsmerkmal dar. Ein nicht vorhandenes Session Timeout gleicht einem erheblichen Sicherheitsrisiko, da die Session wie schon in Kapitel 3.2.2 erläutert, weiterhin bestehen bleibt. Für den Nutzer stellt die visuelle Darstellung dieser Zeitspanne

[76] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S213ff

[77] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S213ff

einen deutlichen Mehrwert und eine Indikation für die Sicherheit der E-Commerce Plattform dar. So werden in der Praxis unter anderem ablaufende Stoppuhren verwendet, welche gut sichtbar angezeigt werden. Möglich ist auch die Verwendung eines eigenen Hinweisfensters, welches dem Nutzer nach einer gewissen Zeitspanne angezeigt wird. Sollte die Webseite aktiv verwendet werden (beispielsweise durch Navigation oder der Aktivierung von Schaltflächen), erhöht sich die verbleibende Zeit automatisch.[78]

3.4. Cookies

Cookies sollten stets auf sichere Art und Weise verwendet werden. Hierfür werden auf der Serverseite bestimmte Flags gesetzt, welche den Grad an Sicherheit kennzeichnen. Neben den im Rahmen des Session Managements aufgezählten Merkmalen wie beispielsweise der Ablauf einer Session ID über entsprechende Parameter nimmt die Übertragungsart der Cookies selbst eine entscheidende Rolle ein. Ein Cookie muss zunächst auf möglichst sicherem Weg vom Server zum Client gesendet werden. Um zu gewährleisten, dass für diesen Kommunikationsweg ausschließlich die verschlüsselte Form verwendet wird, kann der Anbieter einer E-Commerce Plattform verschiedene Markierungen (sogenannte „Flags“) setzen.[79]
Abbildung 7 zeigt die Darstellung der für die IT-Sicherheit relevanten Flags.

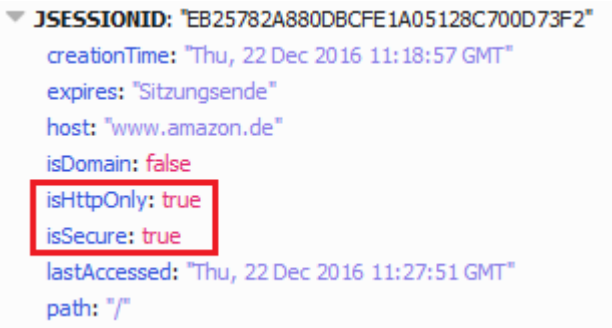


Abbildung 7: Prüfen der gesetzten Cookie Flags[80]

[78] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S213ff

[79] Vgl. Lepofsky R.: The Manager’s Guide to Web Application Security, S30ff

[80] Eigene Darstellung, Screenshot aus: Mozilla Firefox, Version 50.1.0 unter Verwendung des Plugins: Firebug, Version 2.0.18, URL: https://www.amazon.de

Die Überprüfung kann mittels Browser Plugins (in diesem Fall wurde das Plugin Firebug in der Version 2.0.18 verwendet) durchgeführt werden. Plugins stellen nützliche Werkzeuge dar, um auf der Nutzerseite die sichere Übertragung von Cookies zu überprüfen.

Markierung „isHttpOnly“

Die erste Markierung (isHttpOnly) schließt ein Auslesen der Informationen sowohl auf der Client- als auch auf der Serverseite aus. Schadsoftware könnte mittels Browser Erweiterungen wie beispielsweise ActiveX, Adobe Flash oder Java-Applets (vgl. Kapitel 3.6.2.) Daten aus Cookies extrahieren und weiterverarbeiten.

Markierung „isSecure“

Die zweite Markierung (isSecure) gewährleistet die sichere und verschlüsselte Übertragung der Daten. Unverschlüsselte HTTP Anfragen würden die Informationen im Klartext übertragen. Der verwendete Browser ignoriert unsichere Anfragen, ein Abfangen der Informationen kann damit wirkungsvoll verhindert werden.

Ablaufdatum

Zuletzt soll noch auf das Ablaufdatum von Cookies hingewiesen werden. Die Lebensdauer sollte einen verhältnismäßig nachvollziehbaren Zeitraum betragen, und darüber hinaus auch nur solange gültig sein wie es die jeweilige Plattform erfordert.

In Bezug auf die Verwendung einer Session ID kann auch der Wert „Session Only“ gesetzt werden, welcher abläuft sobald der Browser geschlossen wird. Die Inhalte von Cookies lassen sich in modernen Browsern jederzeit einsehen, dies geschieht entweder über ein Symbol direkt in der Adresszeile oder über weiterführende Schaltflächen in den Browser Einstellungen.[81]

3.5. Zertifikate

Die Verifizierung der Echtheit einer Webseite ist für den Nutzer eine wesentliche Voraussetzung, um Betrugsversuche und einen möglichen Diebstahl von vertraulichen Daten zu verhindern. Dies geschieht in der Regel über digitale Zertifikate. Diese werden

[81] Vgl. Lepofsky R.: The Manager’s Guide to Web Application Security, S58f

von einer unabhängigen Zertifizierungsstelle, der sogenannten „Certificate Authority“ (CA) ausgestellt und sollen die Echtzeit einer Webseite garantieren. Die Zertifizierungsstelle prüft die Identität des Anbieters einer Webseite und in weiterer Folge das Zertifikat. Zusätzlich enthält es Informationen zu der Gültigkeit und der eingesetzten Verschlüsselung. Das reine Vorhandensein eines Zertifikats stellt jedoch alleine noch kein Sicherheitsmerkmal dar. Das Angebot an Zertifizierungsstellen ist groß und nicht eingeschränkt, daher ist es für den Nutzer nicht nachvollziehbar wie vertrauenswürdig die jeweilige CA wirklich ist. Es ist für einen Angreifenden ohne weiteres möglich, ein gültiges Zertifikat zu erlangen. In den nachfolgenden Kapiteln sollen daher die wichtigsten Sicherheitsmerkmale von Zertifikaten hervorgehoben und näher erläutert werden.[82]

3.5.1. Zertifikatsfehler

Zertifikatsfehler lassen sich je nach verwendeter Browser Version direkt in der Adresszeile ablesen. Sie weisen auf ein nicht vorhandenes, nicht bestätigtes oder bereits abgelaufenes Zertifikat hin. Dadurch kann die Echtheit einer Webseite nicht mehr garantiert werden, eine Transaktion würde für den Nutzer ein erhöhtes Risiko darstellen. Je nach Browser Version sieht das Dialogfenster unterschiedlich aus.[83]

[82] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S148ff

[83] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S148ff

In Abbildung 8 ist ein ungültiges Sicherheitszertifikat unter Mozilla Firefox ersichtlich.

Abbildung 8: Anzeige eines ungültigen Zertifikats[84]

Hinweise dieser Art erscheinen direkt im Anzeigefenster des Browsers. Der Nutzer muss explizit bestätigen, die Seite dennoch aufrufen zu wollen. Dies sollte nur in Ausnahmefällen geschehen, da ein von Anfang an fehlerhaftes Zertifikat ein wichtiger Indikator für das zu erwartende Sicherheitsniveau einer Webseite ist. Ein bestätigtes Zertifikat wird üblicherweise über einen grün markierten Teil im linken Bereich der Adresszeile dargestellt (vgl. Abbildung 9).[85]

Abbildung 9: Anzeige eines gültigen Zertifikats[86]

In diesem Fall wird dem Nutzer kein Dialogfenster angezeigt.

3.5.2. Extended Validation Zertifikate

Um einen zusätzlichen Grad an Sicherheit zu ermöglichen, wurde ein neuer Standard geschaffen, die sogenannten „Extended Validation Zertifikate“ (EV Zertifikate). Hierbei

---

[84] Eigene Darstellung, Screenshot aus: Mozilla Firefox, Version 50.1.0, URL: https://wiki.chaosradio.ccc.de

[85] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S148ff

[86] Eigene Darstellung, Screenshot aus: Mozilla Firefox, Version 50.1.0, URL: https://www.google.at

erfolgt eine weitaus gründlichere Überprüfung des Anbieters durch die Zertifizierungsstelle. Damit soll verhindert werden, dass Angreiferinnen oder Angreifer in den Besitz von digitalen Zertifikaten kommen. Sobald ein EV Zertifikat vorliegt, kann der Nutzer von der Echtheit der Webseite ausgehen. Browser zeigen ein solches Zertifikat üblicherweise durch die Angabe der Identität zusätzlich zu dem farblich markierten Teil der Adresszeile an.[87]

Zusätzlich kann auch der Zusatz „EV“ in den Zertifikatsdetails abgelesen werden, wie in Abbildung 10 ersichtlich ist. Aus der Abbildung geht auch die grün markierte Identität des Anbieters hervor.

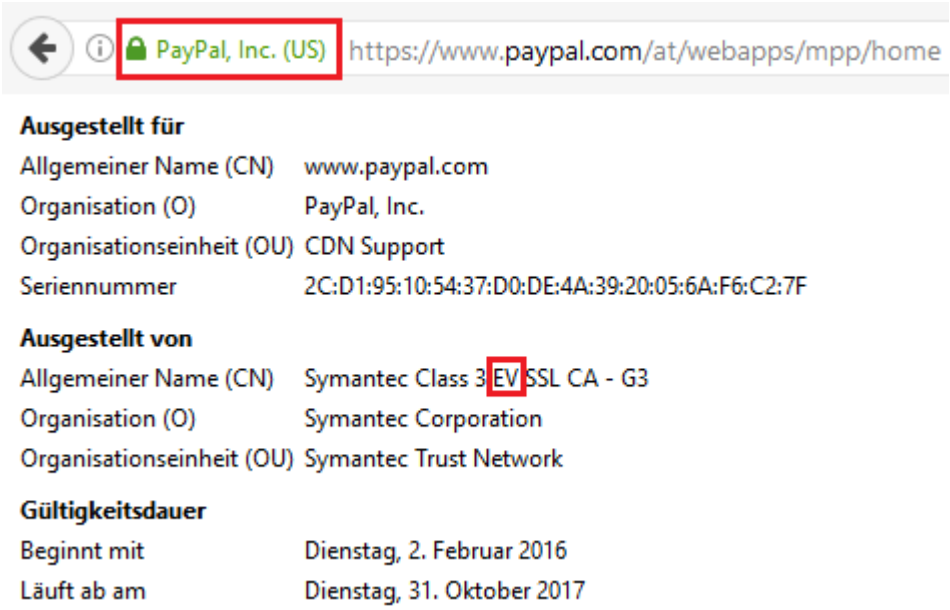


Abbildung 10: Anzeige eines Extended Validation Zertifikats[88]

Um die Übertragungssicherheit, vor allem bei Zahlungsabwicklungen im Rahmen von E-Commerce Transaktionen, zu gewährleisten, sollte in jedem Fall ein gültiges EV Zertifikat vorliegen. Dank moderner Browser kann die Sicherheitsstufe direkt in der Adresszeile abgelesen werden.[89]

---

[87] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S270f

[88] Eigene Darstellung, Screenshot aus: Mozilla Firefox, Version 50.1.0, URL: https://wiki.chaosradio.ccc.de

[89] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S271f

3.6. Browser Erweiterungen

Moderne Browser enthalten eine umfangreiche Auswahl an Erweiterungen (sogenannte „Plugins“). Diese bestehen zunächst aus internen Modulen wie der Möglichkeit, Passwörter zu speichern oder Formulare automatisch zu vervollständigen (vgl. Kapitel 3.6.1.). Darüber hinaus kommt es zu einer Einbettung von Produkten fremder Anbieter, wie beispielsweise JavaScript (Oracle) oder ActiveX (Microsoft). In der Regel stellt die Verwendung von Erweiterungen für den Nutzer ein erhöhtes Sicherheitsrisiko dar. Einige wenige können jedoch auch dabei helfen, den Nutzer auf Sicherheitslücken und sonstige potentiell schädliche Vorgänge hinzuweisen (vgl. Kapitel 3.6.2.).
Die folgenden Kapitel sollen einen Einblick in die Grundlagen der Browser Erweiterungen bieten.

3.6.1. Automatische Speicherung

Die Funktionalitäten der automatischen Speicherung bieten dem Nutzer einen erhöhten Komfort, da sowohl Passwörter als auch persönliche Daten bis hin zu Formulardaten im Speicher des Browsers gehalten werden können, und diese bei Bedarf auch automatisch abrufbar sind. Das größte Risiko stellt hier die Tatsache dar, dass die Daten auch lokal gespeichert werden. Sobald Angreifende also Zugriff auf das lokale System des Nutzers erhalten, könnten diese Daten kopiert werden. Ein weiteres potentielles Risiko stellen Browser Sicherheitslücken dar, durch welche schadhafte Webseiten Zugriff auf Daten erhalten können, welche auf dieser Ebene nicht freigegeben wurden. Um dieses Risiko zu eliminieren, reicht es aus die zugehörige Funktionalität im Browser abzuschalten (der entsprechende Eintrag findet sich in den Einstellungen).[90]

3.6.2. Adobe Flash, ActiveX und Java

Die Verwendung externer Erweiterungen von Drittanbietern stellt ein weiteres Sicherheitsrisiko innerhalb der Browserumgebung dar. Vor allem die Ausführung von Adobe Flash, Java-Applets und der Technologie ActiveX stellt ein erhöhtes Sicherheitsrisiko für den Nutzer dar. Die Angriffsfläche wird erheblich erhöht.[91]

---

[90] Vgl. Lepofsky R.: The Manager’s Guide to Web Application Security, S26

[91] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S281f

Auch der Einsatz von Java, einer populären Programmiersprache, erhöht das Sicherheitsrisiko beträchtlich. Betroffen ist sowohl die Kommunikation mit dem Server als auch die Speicherung von sensiblen Daten auf der Clientebene. In einigen Fällen können ausführbare Objekte als Cookies abgelegt werden (beispielsweise „Flash Cookies“ unter Verwendung von Adobe Flash). Der Programmcode dieser Inhalte kann von Angreifern manipuliert werden. Es ist daher empfehlenswert, diese Module im Browser zu deaktivieren. Alternativ existieren auch Erweiterungen, allen voran JavaScript und HTML5, welche ein weitaus höheres Sicherheitslevel bieten. Dennoch können auch hier Sicherheitslücken auftreten, welche vom Nutzer zumeist nicht bemerkt werden.[92]

Eine Besonderheit stellen Erweiterungen dar, welche den Nutzer auf das vorhandene Sicherheitslevel einer Webseite explizit hinweisen. Dazu zählt unter anderem das Plugin „NoScript“ für Mozilla Firefox. Durch die Verwendung von Tools dieser Art kann die Ausführung von potentiell gefährlichen Inhalten wie Applets oder ActiveX unterbunden werden. Auch bekannte Sicherheitslücken können durch diese Tools an den Nutzer kommuniziert werden, selbst unter Verwendung von modernen Technologien.[93]

3.7. Standards und Gütesiegel

Anerkannte Standards stellen für den Nutzer ein probates Mittel dar, das Sicherheitslevel einer E-Commerce Plattform ohne besondere Kenntnis von technischen Details direkt abzulesen. Seriöse Anbieter erfüllen in der Regel Sicherheitsstandards und weisen dies auch auf der Webseite aus. Nicht alle Standards sind jedoch für den Nutzer erkennbar beziehungsweise relevant für die Sicherheit einer E-Commerce Webseite. So enthalten viele IT-Sicherheitsstandards lediglich Vorgaben für den Einsatz eines Informationssicherheitsmanagementsystems (ISMS). Andere Gütesiegel sind auf die Kennzeichnung von Anbietern, welche Zahlungsabwicklungen durchführen, spezialisiert. Im Rahmen dieser Arbeit soll nur auf für den Nutzer erkennbare Gütesiegel eingegangen werden. Nur diese bringen einen Mehrwert mit sich beziehungsweise ist

[92] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S281f

[93] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S145f

das Fehlen eines oder mehrerer Gütesiegel oftmals ein Indikator für ein erhöhtes Sicherheitsrisiko.[94]
Die folgenden Kapitel sollen einen kurzen Überblick über relevante Standards und Gütesiegel bieten.

3.7.1. PCI-DSS

PCI-DSS steht für „Payment Card Industry – Data Security Standard“. Der Standard wurde von den Kreditkartenfirmen ins Leben gerufen, und steht für eine sichere Abwicklung von Kreditkartentransaktionen. Aktualisierte Versionen und Ergänzungen werden von dem „PCI Security Standards Council“ koordiniert und beschlossen. Zu den Mitgliedern dieses Komitees zählen Delegierte namhafter Kreditkartenanbieter. Die Überprüfung sowie die Zertifizierung ist von der Anzahl der Transaktionen des zu überprüfenden Unternehmens abhängig und reicht von einem Self-Assessment, also einer internen Überprüfung durch eigens dafür abgestellte Angestellte, bis hin zu einem Audit einer unabhängigen dritten Partei. Speziell Schwachstellen im Bereich des E-Commerce sind Bestandteil der umfangreichen Auflagen dieses Standards.[95]

3.7.2. E-Commerce Gütesiegel

Populäre und weit verbreitete Gütesiegel wie beispielsweise Zertifikate stellen ein einfach zu erkennendes Sicherheitsmerkmal für den Nutzer dar. Hiermit soll eine sichere Abwicklung des Bestellprozesses, die Einhaltung von Datenschutzkriterien und die Verwendung von verschlüsselten Kommunikationswegen garantiert werden.

[94] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S120ff

[95] Vgl. Rohr M.: Sicherheit von Webanwendungen in der Praxis, S121ff

Zertifikate können über das Verzeichnis der Anbieter eingesehen werden (vgl. Abbildung 11), zusätzlich befinden sich Symbole im Navigationsbereich der E-Commerce Plattformen.

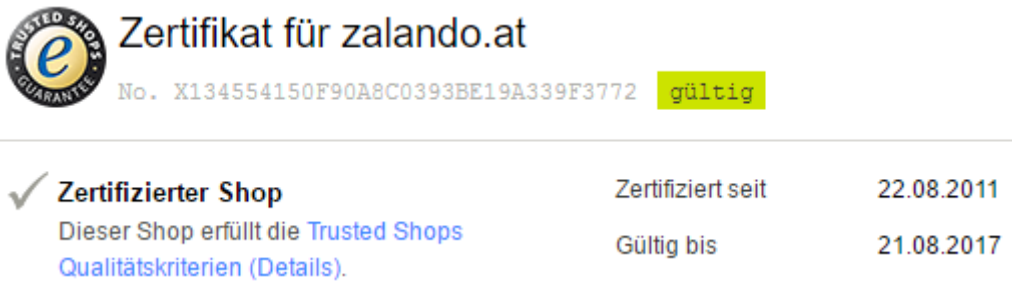


Abbildung 11: Von der Trusted Shops GmbH vergebenes Zertifikat[96]

Kriterien für die Vergabe eines Gütesiegels der Trusted Shops GmbH umfassen auch wichtige Rahmenbedingungen für die Konsumierenden. Dazu zählt eine Liefergarantie, das Recht auf Widerruf beziehungsweise Rücksendung der Ware, der Kundenservice bis hin zu der transparenten Angabe aller Kosten. Auch der Datenschutz fällt in den Wirkungsbereich dieses Anbieters.[97]

[96] Eigene Darstellung, Screenshot aus: Google Chrome, Version 55.0.2883.87, URL: https://www.trustedshops.at/bewertung/info_X134554150F90A8C0393BE19A339F3772.html

[97] Vgl. Trusted Shops Gütesiegel: Die Qualitätskriterien von Trusted Shops, URL: http://www.trustedshops.at/guetesiegel/einzelkriterien.html (abgerufen am 14.12.2016), Trusted Shops GmbH, Köln, 2016

4. Empirie

Nach der Bestimmung und Darstellung aktueller technischer Sicherheitsmaßnahmen auf dem Gebiet der IT-Sicherheit soll in diesem Kapitel die empirische Untersuchung beschrieben, sowie deren Ergebnisse diskutiert werden. Um die Forschungsfrage dieser Arbeit beantworten zu können, wurde eine Online-Umfrage durchgeführt. Das Ziel der Befragung, die Wahl der Befragungsmethode und Methodik sowie der grundsätzliche Aufbau des Fragebogens werden in den nachfolgenden Kapiteln näher dargestellt. Die Auswertung und Interpretation der Daten erfolgt in den beiden abschließenden Kapiteln.

4.1. Hypothese und Ziel der Befragung

Das Ziel der Befragung soll Hinweise darauf geben, wie sich der Fortschritt auf dem Gebiet der IT-Sicherheit auf das tatsächliche Nutzerverhalten auswirkt. Entsprechend lautet die Hypothese dieser Arbeit:

> *„Trotz laufender Verbesserung und Weiterentwicklung der IT-Sicherheit auf dem Gebiet des E-Commerce, sind die tatsächlichen Auswirkungen auf das Nutzerverhalten als gering anzusehen.“*

Um diese Hypothese bestätigen oder verwerfen zu können, bedarf es zunächst einer Erforschung der Wahrnehmung des Nutzers, da diese einen wertvollen Indikator für die Akzeptanz von Sicherheitsmaßnahmen darstellt. Nach diesem einführenden Themenbereich, soll das tatsächliche Nutzerverhalten in zahlreichen Situationen und Zusammenhängen bestimmt werden. Dieser Abschnitt lässt direkte Schlüsse zur Beantwortung der Forschungsfrage zu.
Zusätzlich sollen Zusammenhänge zwischen dem subjektiven Empfinden von IT-Sicherheit und der Realität hergestellt werden. Die Schnelllebigkeit dieses Bereichs kann sehr schnell zu veralteten Wissensständen führen, welches ebenfalls zu einer deutlichen Abweichung zwischen Sicherheitsempfinden und tatsächlicher Sicherheit führen können.

4.2. Methodik

In diesem Kapitel soll zunächst auf die verschiedenen Erhebungsmethoden näher eingegangen werden. Diese werden zunächst in die qualitativen und quantitativen Methoden unterteilt. Im Anschluss daran erfolgt eine Abgrenzung und Begründung der im Rahmen dieser Arbeit gewählten Erhebungsmethode. Abschließend wird die Repräsentativität von Erhebungen im Allgemeinen, sowie von Online-Erhebungen im Speziellen, beleuchtet.

4.2.1. Qualitative Erhebungsmethoden

Qualitative Erhebungsmethoden werden in der Literatur wie folgt definiert:

> *„Qualitative Methoden gehen der Frage nach einzelnen Motiven und Inhalten nach. Sie beschreiben inhaltliche Dimensionen verbal, oft auch interpretativ, erforschen Werte, Gefühle, das „Warum" von Entscheidungen. Im Vordergrund stehen weniger Erhebungsmengen als inhaltliche Tiefe."*[98]

Auf diesem Gebiet lassen sich vor allem das Interview, also eine persönliche Befragung, aber auch die Gruppendiskussion nennen.

Das Interview ist ein systematisch durchgeführtes Gespräch auf fachlicher Ebene, welches in der Regel mit einer zu beforschenden Person geführt wird. Je nach Anforderung können verschiedenste Interviewformen angewandt werden. Beispiele hierfür sind das Experteninterview, oder auch das Tiefeninterview. Bei einem Experteninterview ist die Expertise des Gegenübers zwingende Voraussetzung. Im Vordergrund steht eindeutig das Wissensreservoir, und nicht die Person selbst. Ein Leitfaden hilft der forschenden Person, den roten Faden nicht zu verlieren und alle wesentlichen Inhalte des Forschungsgegenstandes anzusprechen.[99]

Die Gruppendiskussion setzt sich aus mehreren Personen zusammen, welche keinen bestimmten Grad an Expertise aufweisen müssen, um teilnehmen zu können. Hier steht neben der Erforschung von subjektiven Erlebnissen zu einem gewissen Thema auch die soziale Interaktion im Vordergrund. Besonders das Wechselspiel zwischen

---

[98] Braunecker C.: How to do Empirie, how to do SPSS: Eine Gebrauchsanleitung, Stuttgart, 2016, S16

[99] Vgl. Hug T./Poscheschnik G.: Empirisch forschen, Stuttgart, 2014, S104

verschiedenen Meinungen ist Gegenstand dieser Erhebungsmethode. Eine weitere Methode, die teilnehmende Beobachtung, bezieht den Forschenden direkt in die laufende Diskussion ein. Der Vorteil dieser Methode liegt darin, dass neben der Außenperspektive nun auch die Innenperspektive eingenommen werden kann. Des Weiteren kann diese Form der Erhebung in systematische und unsystematische Formen unterschieden werden. Die systematische Form zielt ganz besonders auf bestimmte Verhaltensweisen und Handlungen ab, während die unsystematische Form einer sehr offenen Beobachtungsweise entspricht.[100]

4.2.2. Quantitative Erhebungsmethoden

Quantitative Erhebungsmethoden werden in der Literatur wie folgt definiert:

> *„Quantitative Methoden verfolgen den Ansatz, zu zählen: also nicht verbal auszuformulieren, sondern rein zahlenmäßig zu quantifizieren und daraus Interpretationen abzuleiten. Quantitative Forschung entdeckt keine (weiteren) neuen Zugänge zu einem Thema (höchstens am Rande). Sie arbeitet vielmehr mit bereits vor der Erhebung festgelegten Antwortalternativen bzw. möglichen Ergebnisausprägungen.“*[101]

Durch den Einsatz von quantitativen Erhebungsmethoden wird zunächst versucht, einen Anspruch auf Repräsentativität zu erheben. Speziell durch das Sammeln von größeren Fallzahlen soll dies ermöglicht werden. Dadurch grenzen sich die quantitativen Erhebungsmethoden klar von den qualitativen Methoden ab. Durch den Versuch, Anspruch auf Repräsentativität zu erheben, lassen sich die Ergebnisse in weiterer Folge auch generalisieren. Voraussetzung für eine quantitative Erhebung ist die Messung zählbarer Eigenschaften.

Eine Methode der quantitativen Erhebungsmethoden, welche auch als Methode für die Beantwortung der Forschungsfrage dieser Arbeit gewählt wurde, stellt die Befragung dar. Eine Befragung kann sowohl schriftlich als auch mündlich erfolgen. Die mündliche Befragung ist allerdings stets mit dem Problem der gegenseitigen Beeinflussung konfrontiert. Zusätzlich ist es nur schwer möglich, ausreichende Teilnehmerzahlen zu

---

[100] Vgl. Hug T./Poscheschnik G.: Empirisch forschen, S107ff

[101] Braunecker C.: How to do Empirie, how to do SPSS, S17

erreichen. Die schriftliche Erhebung, zumeist in Form eines Fragebogens, ist im Vergleich günstiger in der Durchführung, aber auch schneller. Zusätzlich lässt sich die Anonymität der Teilnehmenden sowie deren Unbefangenheit bezüglich einer möglichen Beeinflussung sicherstellen. Nachteile liegen vor allem in der fehlenden Möglichkeit, den Antwortprozess nicht kontrollieren zu können. Auch Unklarheiten können bei einer schriftlichen Befragung nicht, oder nur sehr schwer, ausgeräumt werden.[102]

4.2.3. Online-Erhebung

Die Online-Erhebung stellt eine Form der schriftlichen Befragung im Rahmen einer quantitativen Erhebung dar. Bezeichnend für eine Online-Erhebung ist ein Fragebogen, welcher unverändert an einen größeren Personenkreis verteilt wird. Die Online-Erhebung vereint viele Vorteile von empirischen Untersuchungen, welche letztendlich ausschlaggebend für die Auswahl dieser Methode für diese Arbeit waren. Als Hauptmerkmal lässt sich die Tatsache anführen, dass im Vergleich zu alternativen Methoden eine große Stichprobe in relativ kurzer Zeit und unter sehr geringen Kosten erzielt werden kann. Auch offene Fragen können ohne zusätzliche Aufwendungen wie beispielsweise der Transkription gestellt und ausgewertet werden. Eine erhöhte Datenqualität lässt sich durch Kontrolle der gesammelten Daten bereits während der Erhebungsphase sicherstellen. Dies erfordert keinen besonderen Zwischenschritt. Die räumliche und zeitliche Unabhängigkeit stellt eines der wichtigsten Vorteile von Online-Erhebungen dar. Teilnehmende können unabhängig von Ihrem derzeitigen Aufenthaltsort und der aktuellen Zeit an der Umfrage teilnehmen. Abschließend ist auch der gesamte Prozess der Datenerhebung einsehbar und nachvollziehbar. Dadurch können die Ergebnisse von wissenschaftlichen Untersuchungen zusätzlich abgesichert werden.[103]

Aus den eben genannten Gründen wurde für diese Arbeit als Datenerhebungsmethode der Online-Fragebogen gewählt. In Kapitel 4.3. wird auf den grundsätzlichen Aufbau des Fragebogens näher eingegangen, während in Kapitel 4.4. die Durchführung und Diskussion behandelt wird.

---

[102] Vgl. Hug T./Poscheschnik G.: Empirisch forschen, S110ff

[103] Vgl. Kuckartz U./Ebert T./Rädiker S./Stefer C.: Evaluation online: Internetgestützte Befragung in der Praxis, Wiesbaden, 2009, S110f

4.2.4. Stichprobe und Repräsentativität

Ein wichtiges Merkmal jeder Umfrage stellt die Auswahl der Zielgruppe dar. Als Basis jeder Erhebung kommt es hierbei zunächst zu der Definition der Grundgesamtheit. Die Grundgesamtheit wird in der Literatur wie folgt definiert:

> *„Die Grundgesamtheit ist die Menge aller gleichartigen Objekte (Untersuchungseinheiten mit gleichen Ausprägungen von sachlichen, räumlichen und zeitlichen Merkmalen), auf die sich eine empirische Erhebung bezieht. Sie wird auch „Universum", „Population" oder „Kollektiv" genannt."*[104]

Die Grundgesamtheit kann weiters in eine offene oder geschlossene Grundgesamtheit unterteilt werden. Die geschlossene Grundgesamtheit stellt eine abzählbare und definierbare Gruppe von Menschen dar. Im Rahmen dieser Arbeit, welche auf die E-Commerce nutzende weibliche und männliche Bevölkerung Österreichs ab 16 Jahren ausgerichtet ist, kann daher von einer offenen Grundgesamtheit ausgegangen werden. Es ist nicht möglich, den Personenkreis einer abzählbaren Gruppe zuzuordnen. Dieser Umstand hat direkte Auswirkungen auf die Repräsentativität der Erhebung, aber auch auf die Auswahlverfahren der verschiedenen Stichprobenvarianten.[105]
Nach der Festlegung der Grundgesamtheit ist weiters zwischen einer Vollerhebung und einer Stichprobe zu unterscheiden. Die Vollerhebung erfasst alle Teile der definierten Grundgesamtheit, während für die Stichprobe ein repräsentativer Teil stellvertretend für alle erhoben wird. Eine Vollerhebung ist nur in Fällen von kleinen und überschaubaren Bevölkerungs- oder Personengruppen möglich, und kann daher für diese Arbeit nicht in Betracht gezogen werden. Nachfolgend sollen die verschiedenen Möglichkeiten der Stichprobenverfahren vorgestellt und bezugnehmend auf diese Arbeit bewertet werden.[106]

Zufallsgesteuerte Stichprobe

Die zufallsgesteuerten Verfahren sind dadurch gekennzeichnet, dass alle Mitglieder der jeweiligen Grundgesamtheit die Chance erhalten, in die Stichprobe aufgenommen zu

---

[104] Braunecker C.: How to do Empirie, how to do SPSS, S37

[105] Vgl. Kuckartz U./Ebert T./Rädiker S./Stefer C.: Evaluation online, S51

[106] Vgl. Braunecker C.: How to do Empirie, how to do SPSS, S39ff

werden. Dies setzt jedoch eine geschlossene Grundgesamtheit voraus, welche für die Erforschung der Hypothese dieser Arbeit nicht definiert werden konnte. Die Ziehung der Stichprobe selbst muss auf dem Zufall basieren. Hilfreich in der Durchführung ist das Vorhandensein von Verzeichnissen oder auch Listen, aus welchen mit Hilfe eines Zufallsgenerators die Stichprobe zusammengestellt werden kann.

Nicht zufallsgesteuerte Stichprobe

Die nicht zufallsgesteuerten Verfahren können in die Gruppe der bewussten und in die Gruppe der willkürlichen Verfahren unterteilt werden. Die bewusste Auswahl setzt die Festlegung von Kriterien voraus, welche anhand von Listen und festgelegten Regeln erfolgen. Die willkürliche Auswahl, auch Selbstselektion genannt, ermöglicht die Teilnahme an der Erhebung unabhängig einer systematischen Vorauswahl. Eine Online-Erhebung entspricht einer solchen Methode, wobei im Rahmen dieser Arbeit auch Elemente der bewussten Auswahl zur Anwendung gelangten. Durch eine Kriterienfestlegung konnten die selbst selektierten Teilnehmer auf die gewünschte Personengruppe eingeschränkt werden. Dennoch ergeben sich Nachteile dieser Erhebungsmethode, insbesondere für die Repräsentativität der Daten.[107]

Nach der Festlegung der Stichprobenziehung auf ein nicht zufallsgesteuertes Verfahren unter Selbstselektion, musste die Repräsentativität dieser Erhebung eingeschränkt werden. Repräsentativität wird in der Literatur zunächst wie folgt definiert:

> *„Eine Stichprobe ist repräsentativ, wenn sie ein exaktes, lediglich verkleinertes strukturelles Abbild der Grundgesamtheit darstellt. Ziel einer Repräsentativ-Stichprobe ist es, anhand einer kleinen Zahl von Untersuchungseinheiten Aussagen über die Grundgesamt zu treffen“*[108]

Wie aus dieser Definition bereits hervorgeht, kann aufgrund der offenen Grundgesamtheit sowie der willkürlichen und nicht zufallsgesteuerten Stichprobe für diese Arbeit keine Repräsentativität erlangt werden. Einer der Gründe hierfür liegt auch in der Abwicklung der Erhebung selbst. Durch die Verteilung des Links, welcher zur Online-Umfrage führt, über E-Mail, Diskussionsportale und weiteren offenen Kanälen

---

[107] Vgl. Kuckartz U./Ebert T./Rädiker S./Stefer C.: Evaluation online, S51f

[108] Braunecker C.: How to do Empirie, how to do SPSS, S42

können gewisse Faktoren nicht ausgeschlossen werden. Hierzu zählen unter anderem die mehrmalige Teilnahme oder die Überprüfung der wahrheitsgemäßen Angabe der erhobenen Daten. Aus diesen Gründen ergeben sich für eine Online-Erhebung unter einer offenen Grundgesamtheit lediglich Rückschlüsse auf Trends und Beobachtungen unter der Annahme, dass die eingegebenen Daten der Wahrheit entsprechen.[109]
Nachdem in diesem Kapitel die Methodik der Erhebung vorgestellt sowie alternative Methoden diskutiert und abgegrenzt wurden, soll im nun folgenden Kapitel die Gestaltung und der grundsätzliche Aufbau des verwendeten Fragebogens beleuchtet werden. Auch die Durchführung der Befragung ist Gegenstand dieses Kapitels.

4.3. Fragebogen

Für die Gestaltung des Fragebogens galt es zunächst, wichtige wissenschaftliche Rahmenbedingungen und Richtlinien einzuhalten. Nach der Konzeption der verschiedenen Module und Untergruppen konnten die für die Beantwortung der Forschungsfrage relevanten Fragen erstellt und in weiterer Folge zugeordnet werden. Den Abschluss dieses Kapitels bildet eine Übersicht über die verwendeten Tools und Portale sowie Detailinformationen zu der Durchführung der Befragung. Zusätzlich befindet sich der zur Anwendung gelangte Fragebogen in seiner vollständigen Form im Anhang.

4.3.1. Gestaltung des Fragebogens

Die Gestaltung eines Fragebogens, speziell in der Variante einer Online-Erhebung, ist an die allgemeinen Standards für Ethik und Datenschutz geknüpft. Hervorzuheben sind in diesem Zusammenhang vor allem die Teilaspekte der Freiwilligkeit, Vertraulichkeit und der Anonymität. Das Prinzip der Freiwilligkeit umfasst die gänzlich freiwillige Teilnahme an einer Erhebung. Auch die Beendigung beziehungsweise der Abbruch einer bereits begonnenen Teilnahme soll jederzeit und ohne Angabe von Gründen ermöglicht werden.[110]

---

[109] Vgl. Braunecker C.: How to do Empirie, how to do SPSS, S46ff

[110] Vgl. Kuckartz U./Ebert T./Rädiker S./Stefer C.: Evaluation online, S57ff

Das Prinzip der Vertraulichkeit umfasst hauptsächlich den Bereich des Datenschutzes, und damit in erster Linie die Tatsache, dass keine Daten an Dritte weitergegeben werden. Dem Prinzip der Anonymität wird im Rahmen von Online-Umfragen ein besonderer Stellenwert eingeräumt. So wird elektronischen Einladungen und Online Links grundsätzlich ein gewisses Misstrauen entgegengebracht. Absolute Anonymität kann nur sehr schwer erreicht werden, da sowohl die Verteilung der Links auf gewissen Plattformen als auch die Einladung über E-Mail Listen bereits das Prinzip der absoluten Anonymität verletzt. Entscheidend ist jedoch nicht, ob die Einhaltung der aufgezählten Grundprinzipien zugesichert wurde, sondern vielmehr die Tatsache, dass seitens des Forschers alle möglichen Maßnahmen ergriffen wurden.[111]

Die Offenlegung der Einhaltung wurde im Rahmen der Einleitung des Fragebogens bekanntgegeben. Bei der grundlegenden Konstruktion des Fragebogens wurde auf eine aussagekräftige Einleitung, die Formulierung und Technik der verwendeten Fragen sowie auch auf negative Antworttendenzen großer Wert gelegt. So umfasst die Einleitung neben einer kurzen Darstellung der Person und Einrichtung auch Hinweise auf Zusicherung der Anonymität und des Datenschutzes. Die grobe Darstellung des Forschungsinhalts sowie der Fragestellung zählen ebenfalls dazu. Die konzipierten Fragen umfassen das dichotome Antwortformat, Ratingskalen unter verschiedenen Abstufungen bis hin zu offenen und geschlossenen Fragen. Negative Antworttendenzen wie beispielsweise die absichtliche Verstellung, die soziale Erwünschtheit, die sogenannte „Ja-Sage-Bereitschaft“ und auch die Beeinflussung durch die Wahl der Antwortmöglichkeiten wurden vermieden.[112]

4.3.2. Aufbau des Fragebogens

Der Fragebogen wurde mit dem Online Tool SosciSurvey erstellt, und grundsätzlich in verschiedene Teile gegliedert. Nachfolgend sollen die jeweiligen Themenblöcke sowie ausgewählte Fragen vorgestellt, und deren Bedeutung für die Beantwortung der Forschungsfrage näher erläutert werden.

---

[111] Vgl. Kuckartz U./Ebert T./Rädiker S./Stefer C.: Evaluation online, S57ff

[112] Vgl. Raab-Steiner E./Benesch M.: Der Fragebogen: Von der Forschungsidee zur SPSS-Auswertung, Stuttgart, 2015, S54ff

4.3.2.1. Einleitung

Die erste Seite des Fragebogens erscheint direkt nach dem Aufruf der in der Einladung enthaltenen Links. Neben kurzen Informationen zu Bildungseinrichtung, persönlichen Daten und dem eigentlichen Thema dieser Arbeit finden sich auch Hinweise zu der erwarteten Zeitspanne der Umfrage sowie eine Danksagung für die Teilnahme. Das Angebot, auf Rückfrage per E-Mail gerne weitere Informationen zu dem Thema zuzusenden, schließen diesen einleitenden Block ab.

4.3.2.2. E-Commerce Nutzung und Risikowahrnehmung

Der erste große Themenbereich behandelt zunächst den Grad der Nutzung von E-Commerce im Allgemeinen.

> *„Wie häufig haben Sie das Internet innerhalb der letzten 12 Monate für den Kauf von Gütern oder Dienstleistungen genutzt?“*

In der eingehenden Frage, wie oft und ob das Internet innerhalb der letzten 12 Monate für den Kauf von Gütern oder Dienstleistungen verwendet wurde, findet sich auch ein Teil der bewussten Auswahl wieder (vgl. Kapitel 4.2.4.). Wird an dieser Stelle angegeben, E-Commerce nicht zu nutzen, wird auch der Fragebogen unter einer einzelnen Zwischenfrage und den jeweiligen soziodemographischen Aspekten direkt beendet. Dadurch kann eine Selektion erreicht werden, sodass nur aktive E-Commerce Erfahrungen Einzug in die Datenerhebung finden.
Der Hauptteil dieses Themenblocks behandelt Fragen nach dem Grad der Nutzung, der persönlich empfundenen Vor- und Nachteile von E-Commerce bis hin zu der Risikowahrnehmung der Teilnehmer.

> *„Welche Vorteile des E-Commerce stellen für Sie persönlich eine Motivation dar, Online einzukaufen?“*

Diese Frage zielt auf die in Kapitel 2.4.3. erwähnten Nutzenpotentiale ab und soll einen Überblick geben, welche der behandelten Vorteile für den Nutzer relevant sind.

Als Folgefrage werden auch die Nachteile von E-Commerce (vgl. Kapitel 2.4.4.) behandelt.

> *„Welche Nachteile des E-Commerce haben Sie bereits erfolgreich von einem Kauf abgehalten?“*

Besondere Relevanz für die Beantwortung der Forschungsfrage liegt vor allem in den Antwortmöglichkeiten der unsicheren Verbindung sowie der Angst vor Datendiebstahl und Verletzungen im Bereich des Datenschutzes.
Das Kapitel 2.5., welches die Zahlungsabwicklung umfasst, stellt die Grundlage für die Frage nach den genutzten Bezahlmöglichkeiten dar. Durch die Angabe der persönlich favorisierten Methode können Rückschlüsse auf das Sicherheitsbewusstsein der Befragten gezogen werden.

> *„Welche Bezahlmöglichkeiten bevorzugen Sie im Rahmen einer Online Transaktion?“*

Die darauffolgende Frage, sofern als Bezahlvariante die Kreditkarte angegeben wird, richtet sich an die Akzeptanz und Priorisierung der angebotenen Sicherheitsverfahren, darunter TAN/Secure Code oder ähnliche anbieterspezifische Methoden.
Die abschließende Frage dieses Bereichs behandelt konkrete Gründe, wieso von einem geplanten Kauf beziehungsweise einer Transaktion tatsächlich abgesehen wird.

> *„Welche Faktoren stellen für Sie persönlich Gründe dar, von einem Online Kauf abzusehen?“*

Neben möglichen Gründen wie beispielsweise dem Versandrisiko oder der mangelnden Reputation des Anbieters, sind vor allem sicherheitsrelevante Bereiche wie der Datenschutz und unsichere Bezahlmöglichkeiten für diese Studie relevant.

4.3.2.3. Authentifizierung

Der Bereich der Authentifizierung umfasst unter anderem die Nutzung der verschiedenen Methoden, oder auch die Frage nach den bevorzugten und vermiedenen Technologien in Verbindung mit Anmeldung und Passwortsicherheit. Individuelle Daten wie beispielsweise die bevorzugte und praktizierte Mindestanforderung an ein Passwort, die Zeitspanne der freiwilligen sowie nicht-freiwilligen Änderung von Passwörtern und die Einschätzung bezüglich Passwortstärke von vorgegebenen Beispiel Passwörtern

liefern wichtige Erkenntnisse zum Nutzerverhalten und der sich daraus ergebenden Sicherheitsstufe.
Die einleitende Frage richtet sich zunächst an die Nutzung der verschiedenen Authentifizierungsmethoden.

> *„Welche Authentifizierungsmethode(n) bevorzugen Sie, jeweils zusätzlich zu Benutzername bzw. E-Mail Adresse?“*

Hiermit soll in Erfahrung gebracht werden, welche Authentifizierungsmethoden in welcher Kombination und Anzahl genutzt werden. Das Spektrum reicht von einer einzelnen Methode wie beispielsweise dem Passwort bis hin zu der Nutzung von sämtlichen zur Verfügung stehenden Methoden. Da die Authentifizierung, wie in Kapitel 3.2. ausführlich dargestellt, einen sehr hohen Stellenwert in der IT-Sicherheitskette einnimmt, ist dieser Themenbereich für die Beantwortung der Forschungsfrage von hoher Relevanz.

> *„Nutzen Sie eine E-Commerce Plattform dennoch, auch wenn diese nicht Ihrer bevorzugten Authentifizierungsmethode entspricht?“*

Aufschlussreich in Bezug auf das tatsächliche Nutzerverhalten ist die Frage nach der Vorgehensweise, wenn die bevorzugte Authentifizierungsmethode nicht zur Verfügung stehen sollte. Die Nutzung der jeweiligen Plattform, selbst unter einem Mangel an Alternativen, führt zu wichtigen Erkenntnissen.
Die folgenden Fragen behandeln das Thema Passwortsicherheit (vgl. Kapitel 3.2.1.) und beinhalten verschiedene Mindeststandards der Befragten.

> *„Wie schätzen Sie die Passwortstärke Ihrer eigenen Passwörter ein?“*
> *Welche Eigenschaften der von Ihnen verwendeten Passwörter sind für Sie ein unverzichtbarer Bestandteil?*
> *Wie viele Zeichen entsprechen Ihren persönlichen Passwort-Mindestanforderungen?*

Eine Kombination aus mehreren Fragen zu diesem Thema lässt auf mögliche Widersprüche zwischen der Einschätzung der eigenen Passwortstärke und der Kriterien für ein sicheres Passwort schließen.

Die Frage nach der freiwilligen oder auch unfreiwilligen Änderung von Passwörtern ist ein weiterer Indikator für die Nutzerwahrnehmung. Abschließend wird den Befragten eine Reihe von Beispiel Passwörtern präsentiert, welche auf eine Zeitspanne bis zu einem erfolgreichen Angriff eingeschätzt werden sollen. Dadurch soll die Verbindung zwischen der angegebenen Sicherheit der eigenen Passwörter und der Wahrnehmung der Passwortsicherheit anhand von Beispielen hergestellt werden.

4.3.2.4. Session Management und Cookies

Dieser Themenbereich erweitert die Einschätzung des Nutzerverhaltens mittels der Feststellung von Übertragungstechnologien, dem Bewusstsein über aktuell technisch mögliche Angriffsszenarien und Bedrohungen auf diesem Gebiet und dem grundsätzlichen Verständnis von wichtigen Tools der IT-Sicherheit wie beispielsweise der Verwendung von Cookies und Zertifikaten. Tiefere Einblicke sollen einzelne Folgefragen zu diesem Bereich geben, welche vor allem den realen – im Gegensatz zu dem empfundenen – Grad an Sicherheit messen sollen.
Wie in Kapitel 3.2.3. erläutert, stellt die Verwendung einer HTTPS Verbindung eine wichtige Grundlage für die Verwendung von E-Commerce dar.

> *„Achten Sie auf eine sichere Verbindung im Browser, sobald Sie eine E-Commerce Plattform nutzen?“*

Durch diese Frage kann in Erfahrung gebracht werden, ob explizit auf eine HTTPS Verbindung geachtet wird. Eine zusätzliche Antwortmöglichkeit erfasst, ob bewusst kein Wert auf die Verbindungsart gelegt wird, oder ob die Information schlichtweg nicht bekannt ist.

> *„Sofern Sie eine HTTPS Verbindung erkennen, auf welche Art überprüfen Sie die Gültigkeit der Verbindung?“*

Die Folgefrage behandelt die Art der Überprüfung einer gültigen Verbindung. Nur die Kombination aus diesen beiden Fragen lässt gültige Rückschlüsse zur Beantwortung der Forschungsfrage zu.

Der zweite Teil dieses Bereichs behandelt die Möglichkeit, eine komplette „Session“, also Login/Passwort sowie Warenkorb durch einen Angriff zu übernehmen. Weitere Fragen umfassen die Verwendung von Cookies sowie die Begründung, falls diese abgelehnt werden sollten.

„Wie lautet Ihre Meinung zu der Verwendung von Cookies im Rahmen von E-Commerce Transaktionen?“
Aus welchen Gründen lehnen Sie die Verwendung von Cookies ab?“

Speziell die Gründe für eine potentielle Ablehnung geben wertvolle Hinweise auf das tatsächliche Sicherheitsempfinden der Befragten. Wie in Kapitel 3.3. sowie Kapitel 3.4. erläutert, bringt die Verwendung von Cookies zwar ebenfalls Gefahren mit sich, jedoch birgt die Alternative durch den Angriffspunkt der Session ID innerhalb der URL ein noch viel höheres Gefahrenpotential.

„Ist Ihnen die Funktionsweise von Zertifikaten bzw. deren Bedeutung für die Sicherheit einer E-Commerce Plattform bewusst?“

Zertifikate stellen ein probates Mittel dar, die Echtheit einer Webseite verifizieren zu können (vgl. Kapitel 3.5.). Im Rahmen dieser Frage wird Wert darauf gelegt, ob den Befragten die Funktionsweise prinzipiell klar ist, ob diese unzureichende Informationen über Zertifikate besitzen, oder ob kein Interesse an Zertifikaten beziehungsweise deren Überprüfung besteht.

4.3.2.5. Browser Erweiterungen und Gütesiegel

Der Bereich der Browser Erweiterungen und Gütesiegel rundet das Bild dahingehend ab, als dass gängige Hilfsmaßnahmen auf dem Gebiet der IT-Sicherheit wie beispielsweise Browser Plugins, Funktionalitäten und Gütesiegel bewertet und deren Nutzung erhoben werden soll.

„Welche Browser Erweiterungen bzw. Funktionalitäten nutzen Sie regelmäßig?“

Die verschiedenen Browser Funktionalitäten (vgl. Kapitel 3.6.) bieten in erster Linie zusätzliche Angriffspunkte, und nur wenige Maßnahmen zur Erhöhung der IT-Sicherheit. Eine Auswahl an Plugins wird den Befragten angeboten, zusätzlich besteht auch die Möglichkeit einer offenen Eingabe.

Der abschließende Teil dieses Bereichs umfasst die verschiedenen Gütesiegel und deren Akzeptanz sowie Signifikanz.

„Welchen Stellenwert räumen Sie den folgenden Gütesiegeln bei der Verwendung von E-Commerce Plattformen ein?“
Wie überprüfen Sie die Gültigkeit eines Gütesiegels?

Auch hier lässt die Beantwortung der Frage nach der Methodik der Überprüfung eines Gütesiegels wertvolle Rückschlüsse zur Bestätigung beziehungsweise Widerlegung der Hypothese zu. Der Stellenwert eines Gütesiegels stellt aus Sichtweise der IT-Sicherheit noch keine tatsächliche Reduktion des Risikos dar (vgl. Kapitel 3.7.). Nur wenn das jeweilige Gütesiegel auch ausreichend überprüft wird, kann eine Erhöhung der tatsächlichen Sicherheit erzielt werden.

4.3.2.6. Soziodemographische Daten

Dieser abschließende Themenbereich umfasst die Frage nach wichtigen soziodemographischen Daten, um die Aussagekraft dieser Studie noch weiter zu erhöhen. Es wurde bewusst auf eine zu detaillierte Profilerstellung verzichtet, um die Abbruchrate niedrig halten zu können. Zwingende Angaben beinhalten das Geschlecht, die Altersgruppe, den höchsten Bildungsabschluss und den derzeitigen Wohnort. Das monatliche Nettoeinkommen stellt eine optionale Angabe dar und wurde gestaffelt unter verschiedenen Einkommensgrenzen angegeben.

Die letzte Seite des Fragebogens beinhaltet eine kurze Danksagung und den Hinweis, dass Browser-Fenster nun schließen zu können. Auf Anregung verschiedener Pretester soll auch eine kurze Lösung der angebotenen Beispiel Passwörter aus dem Bereich der Authentifizierung und deren Zeitspanne für einen erfolgreichen Angriff veröffentlicht werden.

4.3.3. Durchführung der Befragung

Die Befragung wurde zur Gänze in dem Online Portal SosciSurvey realisiert. Nach der Anlegung der verschiedenen Module und Fragen wurden zunächst personalisierte Links an einzelne Personen verschickt. Die im Rahmen dieses Pretests durchgeführten Erhebungen konnten durch Kommentare ergänzt werden und auf diesem Weg noch letzte Korrekturen und Verbesserungen vorgenommen werden. Nach der erfolgreichen

Pretest Phase wurde die Umfrage über verschiedene Portale, Social-Media-Kanäle und auch über E-Mail geteilt. Der Befragungszeitraum betrug 30 Tage, die Erhebung war zwischen 02.03.2017 und 31.03.2017 aktiv. Nach der Beendigung des Befragungszeitraumes wurden die Antworten in ein Analyse- und Statistiktool übertragen. Eine entsprechende Export Funktion findet sich direkt in dem Portal SosciSurvey. Die Daten wurden vor dem Export auf Vollständigkeit und Fehler überprüft. Unvollständige Datensätze sowie zweifelhafte Teilnahmen auf Grund unrealistischer Zeitspannen wurden verworfen.

4.4. Datenauswertung und Analyse

Die Daten wurden nach dem Export aus SosciSurvey und der anschließenden Überleitung mit dem Statistik- und Analyseprogramm IBM SPSS Statistics in der Version 24 ausgewertet. Die deskriptive Datenanalyse erfolgte über Häufigkeits- und Kreuztabellen unter Zuhilfenahme der verschiedenen programminternen Tools. Filtereinstellungen sowie die Unterscheidung in absolute und relative Häufigkeiten konnte direkt in IBM SPSS vorgenommen werden. Sämtliche Diagramme und Tabellen wurden mit Hilfe von Microsoft Office 365 Pro Plus in der Version 1704 erstellt. Zur Anwendung gelangten die Programme Microsoft Word und Microsoft Excel.
Insgesamt konnten im Untersuchungszeitraum 150 Teilnahmen registriert werden, wovon 20 verworfen werden mussten, da der Fragebogen nicht vollständig ausgefüllt wurde. Vier von den 130 verbleibenden Teilnahmen fanden keine Berücksichtigung in der Beantwortung der Forschungsfrage, da keine aktive E-Commerce Transaktion im Zeitraum der letzten 12 Monate angegeben wurde. Drei von den 126 verbleibenden Teilnahmen fanden keine Berücksichtigung, da sich die teilnehmenden Personen derzeit nicht in Österreich aufhielten. Für die Überprüfung der Hypothese ergibt sich somit ein Teilnehmerfeld von insgesamt 123 Datensätzen.

4.4.1. Charakteristika der Studienteilnehmer

Das **Teilnehmerfeld** enthält 59,3 % Frauen und 40,7 % Männer. In diesem Zusammenhang kann von einer ausgewogenen Verteilung zwischen den Geschlechtern ausgegangen werden. Erwartungsgemäß und anhand der Gesamtbevölkerung

Österreichs bemessen, wurde bereits im Vorfeld von einer höheren weiblichen Teilnehmerquote ausgegangen.

Die **Altersgruppe** findet den größten Anteil im Bereich von 25 bis 34 Jahren. Die nachfolgende Abbildung 12 zeigt die Verteilung der Altersgruppen anhand eines Diagrammes.

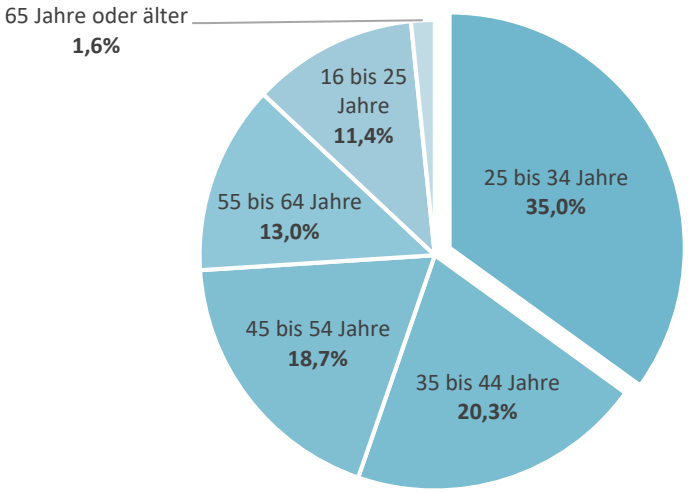


Abbildung 12: Altersgruppen

Für die Erhebung der Nutzerwahrnehmung nimmt der Faktor Alter zwar keine unmittelbar entscheidende Rolle ein, dennoch lassen sich aus den verschiedenen Altersgruppen wichtige Erkenntnisse in Bezug auf den Einsatz und auch die Akzeptanz von IT-Sicherheitsmethoden ableiten.

Die **Bildungsabschlüsse** lassen auf ein allgemein höheres Bildungsniveau schließen, mit 4,9 % an Lehr-, einem Anteil von 43,1 % an Matura- sowie 52 % an Hochschulabschlüssen (vgl. Abbildung 13).

Abbildung 13: Verteilung Bildungsabschlüsse

Entsprechend liegen die erhobenen **durchschnittlichen Einkommen** mit 42,3 % zwischen € 2.000,- und € 2.999,- wobei an zweiter Stelle die Einkommen zwischen € 1.000,- und € 1.999,- erfasst werden konnten.

4.4.2. E-Commerce Nutzung

Bezüglich der Nutzung selbst wurden zunächst die aus Teilnehmersicht relevanten **Vorteile von E-Commerce** bewertet. Die in Kapitel 2.4.3. vorgestellten Nutzenpotentiale aus der Sicht der Konsumierenden wurden im Rahmen der Befragung eindeutig bestätigt. So gab ein kombinierter Anteil zwischen 92,7 % und 99,2 % der Befragten an, die angegebenen Vorteile auch als solche anzuerkennen. Der Vorteil der individualisierten Angebote wurde hierbei von 92,7 % der Befragten als Vorteil gesehen, die Orts- und Zeitunabhängigkeit im E-Commerce sogar mit 99,2 % (vgl. Abbildung 14).

Weitere Vorteile wie beispielsweise verschiedene Liefermethoden, die mobile Nutzungsmöglichkeit bis hin zu der Möglichkeit der erleichterten Informationsbeschaffung und Preisvergleiche lagen jeweils dazwischen.

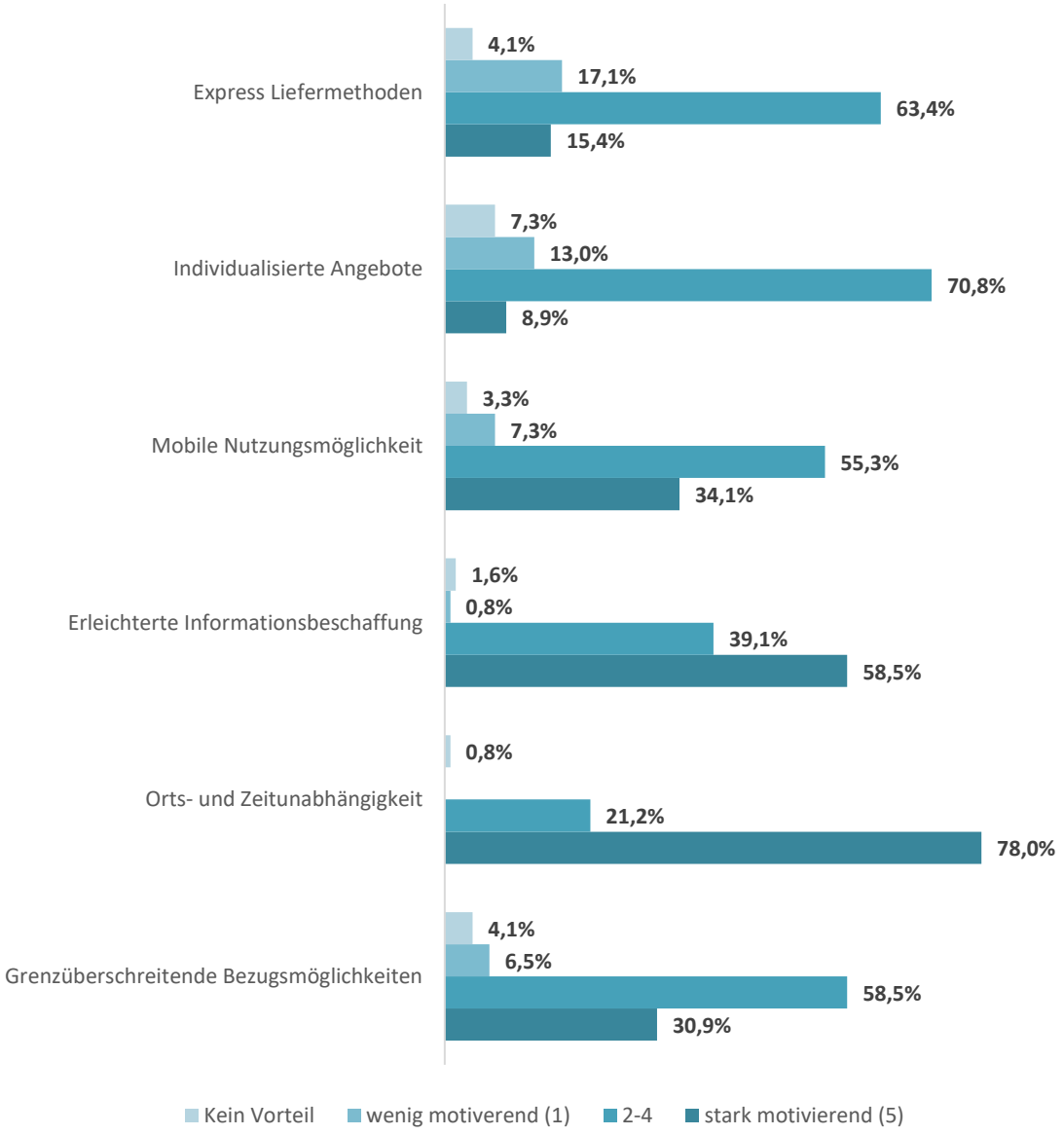


Abbildung 14: Vorteile E-Commerce

Die **Intensität der Nutzung von E-Commerce** kann mit 56,1 % als regelmäßig angegeben werden, wovon 42,3 % mehrmals monatlich und 13,8% mehrmals wöchentlich einkaufen. Die zweite Antwortgruppe in Form von 43,9 % nutzen

E-Commerce dagegen in unregelmäßigen Abständen über mehrere Wochen oder über das gesamte Jahr verteilt.
Die Verteilung der **Nachteile von E-Commerce** können der Abbildung 15 entnommen werden und wurden analog zu Kapitel 2.4.4. strukturiert.

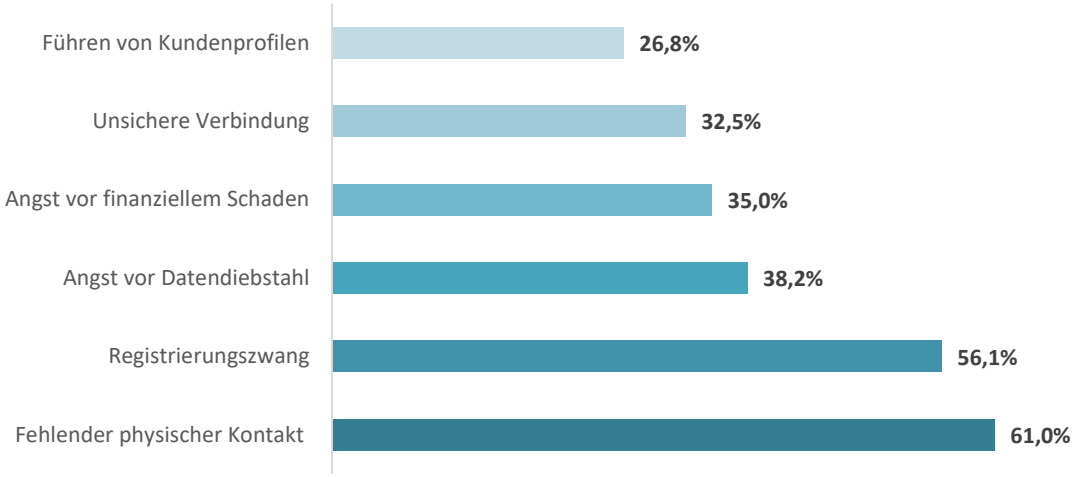


Abbildung 15: Nachteile E-Commerce

Hervorzuheben sei in diesem Zusammenhang der Registrierungszwang sowie der fehlende physische Kontakt mit dem Produkt. Diese Nachteile wurden von jeweils 56,1 % sowie 61 % der Befragten bestätigt. Sehr auffällig für die Kundenwahrnehmung ist der im Vergleich sehr niedrige Wert im Falle der unsicheren Verbindung. Da ein Großteil der IT-Sicherheitsrisiken im Bereich der Verbindung und Authentifizierung liegt würde ein höherer Wert auch einer höheren Awareness entsprechen. Die von den Nutzerinnen und Nutzern wahrgenommenen Nachteile liegen daher klar im Bereich der Produktnähe und der Bequemlichkeit.
Als bevorzugte **Bezahlmethode** kann eindeutig die Kreditkarte und die Verwendung von PayPal angegeben werden. Diese stellen gleichzeitig auch das größte Risiko dar. Die sicheren Methoden wie beispielsweise der Kauf auf Rechnung, Vorkasse oder Lastschrift werden von den Befragten nur sehr selten verwendet (vgl. Abbildung 16).

Detaillierte Angaben zu den verschiedenen Bezahlmöglichkeiten können der nachfolgenden Abbildung 16 entnommen werden.

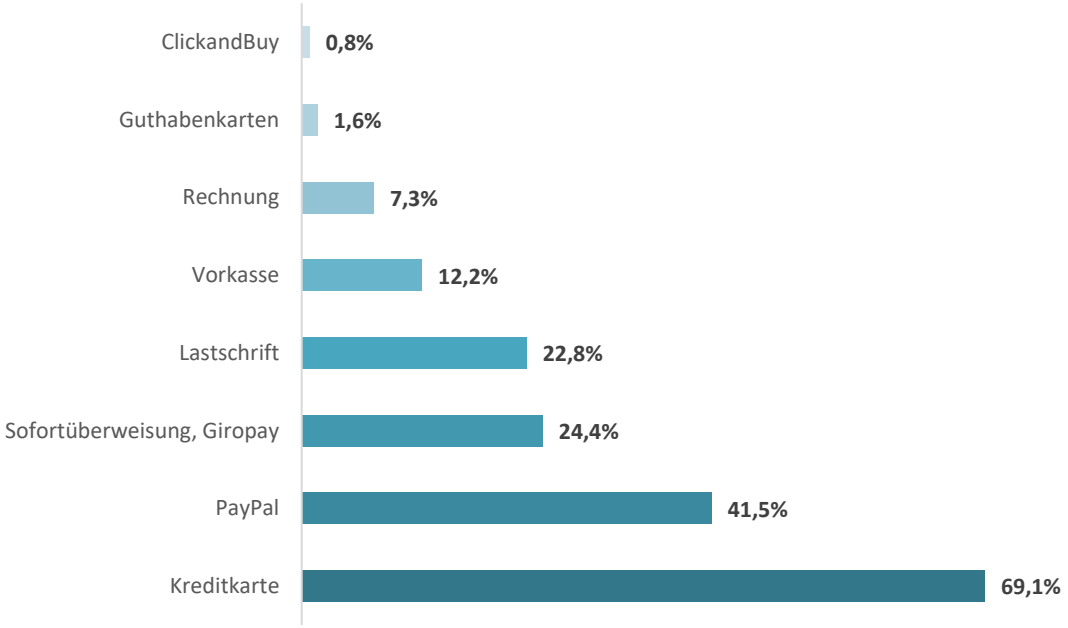


Abbildung 16: Bevorzugte Bezahlmöglichkeiten

Die Folgefrage nach einem **Abbruch bei Kreditkartenzahlung** wurde an insgesamt 88 Befragte gestellt, welche die Kreditkarte als eines der bevorzugten Zahlungsmittel angaben. Falls keine zusätzliche Sicherheitsmethode wie beispielsweise das TAN/Secure Code Verfahren angeboten wird, stellt dies nur für 22,4 % der Befragten einen Abbruchgrund dar. Insgesamt 77,7 % nutzen die jeweilige E-Commerce Plattform dennoch, wobei 22,4 % der Befragten aus dieser Gruppe angaben, nur bei mangelnden Alternativen nicht abzubrechen. Dies ist aus Sichtweise der IT-Sicherheit kein Grund, den Einkauf auf einer potentiell unsicheren Seite fortzusetzen. Das Fehlen einer Alternative ist für sich alleine kein Argument für eine unsichere Transaktion. Eine Kreditkartenzahlung ohne Eingabe eines zusätzlichen PIN Codes oder einem Passwort lässt in den meisten Fällen auf ein niedrigeres Sicherheitsniveau schließen.

4.4.3. Risikowahrnehmung

Die Risikowahrnehmung wurde anhand zweier Fragen in Bezug auf Kapitel 3.1. erhoben. Zunächst mussten **Tendenzen** bezüglich der persönlichen Online Kauferfahrung, der Zufriedenheit und dem Selbstvertrauen im Umgang mit E-Commerce und einige weiter Faktoren erhoben werden. Die **Online Kauferfahrung** wurde von 80,5 % der Befragten als überdurchschnittlich beziehungsweise hoch eingestuft. Für die Wahrnehmung und Selbsteinschätzung sehr wichtig gilt der Wert des **Selbstvertrauens** in den persönlichen Umgang mit E-Commerce. Hier gaben 78,9 % der Befragten an, ein hohes Selbstvertrauen zu besitzen. Nur 6,5 % gaben an, ein eher niedriges Selbstvertrauen gegenüber E-Commerce Transaktionen mitzubringen (vgl. Abbildung 17).

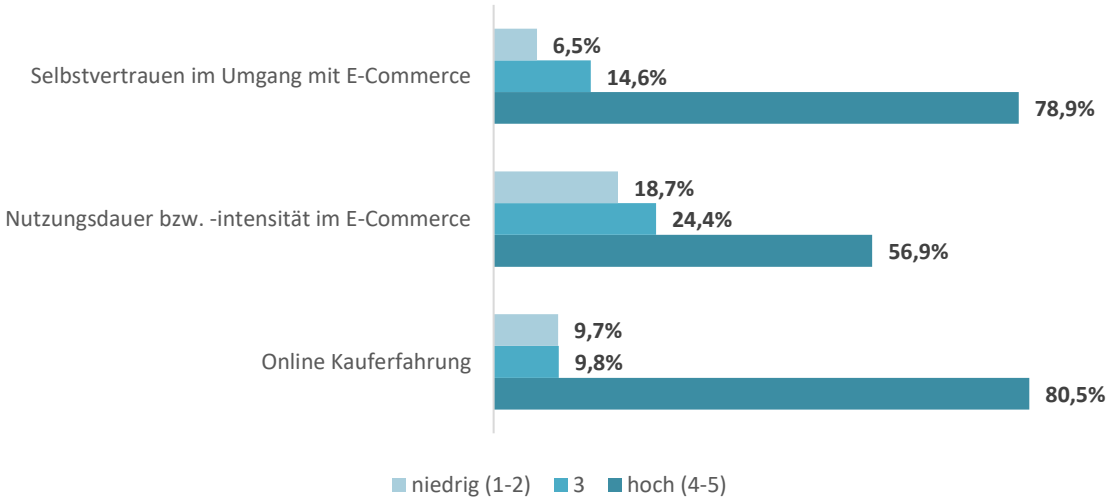


Abbildung 17: Einschätzung der Befragten bezüglich E-Commerce Nutzung

Bei der Gegenüberstellung der Daten kann ein **Zusammenhang** zwischen der Nutzungsdauer beziehungsweise -intensität und dem Selbstvertrauen beobachtet werden. Mit steigender Nutzungsdauer steigt prinzipiell auch das Selbstvertrauen, jedoch gaben speziell im Bereich der niedrigen Nutzungsdauer (Skalenpunkte 1-2, 23 Befragte) eine Gruppe von 60,9 % an, dennoch ein hohes Selbstvertrauen zu besitzen (Skalenpunkte 4-5).

Die Frage nach **Faktoren**, welche von einem Online Kauf prinzipiell abschreckend wirken, wurde vor allem im Bereich der IT-Sicherheit sehr gemischt geantwortet. So gaben nur 22 % der Befragten an, dass Datenschutz ein persönliches Risiko darstellt. Unsichere Bezahlmöglichkeiten wurde von 36,6 % als Risiko, und damit abschreckend, eingestuft (vgl. Abbildung 18).

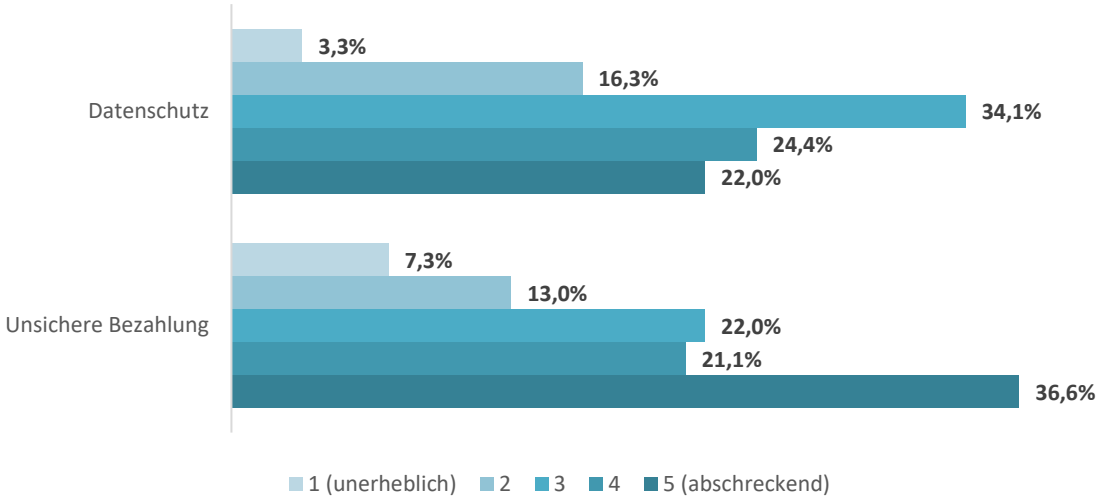


Abbildung 18: Unsichere Bezahlung und Datenschutz

Abschließend kann festgestellt werden, dass die Risikowahrnehmung seitens der Befragten als niedrig einzustufen ist. Die tatsächliche Aussage dieser Werte wird jedoch erst durch die weitere Analyse im Zuge der nachfolgenden Themengebiete deutlich.

4.4.4. Authentifizierung

Die zur Anwendung gelangenden Authentifizierungsmethoden stellen ein wesentliches Merkmal einer sicheren und geschützten Transaktion dar. Um die eingesetzten Methoden sowie die Wahrnehmung der Befragten diesbezüglich zu erheben, wurden insgesamt neun Fragen gestellt, welche neben der Anmeldung selbst auch die verwendete Passwortstärke sowie die Einschätzung von vorgegebenen Passwörtern umfasste.

Als bevorzugte **Authentifizierungsmethode** nutzen 87,8 % der Befragten das Passwort, auf dem zweiten Platz folgt die Nutzung eines Tokens mit 57,7 %. Biometrie wird nur von 15,4 % aller Teilnehmerinnen und Teilnehmer genutzt (vgl. Abbildung 19).

Abbildung 19: Bevorzugte Authentifizierungsmethode

Bezüglich der Anzahl der **gleichzeitig verwendeten Methoden** gaben jeweils 46,3 % der Befragten an, eine oder zwei Methoden gleichzeitig zu verwenden. Das volle Ausmaß von drei verwendeten Methoden erreichen 7,3 %.

Ausgehend von den 46,3 % der Befragten, welche zwei Methoden gleichzeitig verwenden, konnte die **Kombination Passwort und Token** mit 86 % als eindeutig bevorzugte Methode festgestellt werden. Dies entspricht aus der Sichtweise der IT-Sicherheit einem erwünschten Ergebnis, wobei die Passwortstärke einen maßgeblichen Anteil an der tatsächlich erzielten Sicherheitsstufe trägt.

Die Frage nach der Nutzung einer Plattform, obwohl die bevorzugte Authentifizierungsmethode nicht zur Verfügung steht, wurde von insgesamt 69,9 % aller Befragten bestätigt. Hiervon gaben 38,2 % an, die Plattform nur unter unzureichenden Alternativen zu nutzen (vgl. Abbildung 20).

Rund ein Drittel lehnen die Nutzung kategorisch ab. Diese Zahlen lassen – analog zu der Frage nach dem Kaufabbruch bei Kreditkartenzahlung – auf ein geringes Sicherheitsbewusstsein schließen. Der Kauf oder die Nutzung eines Portals darf unter keinen Umständen im Vordergrund stehen.

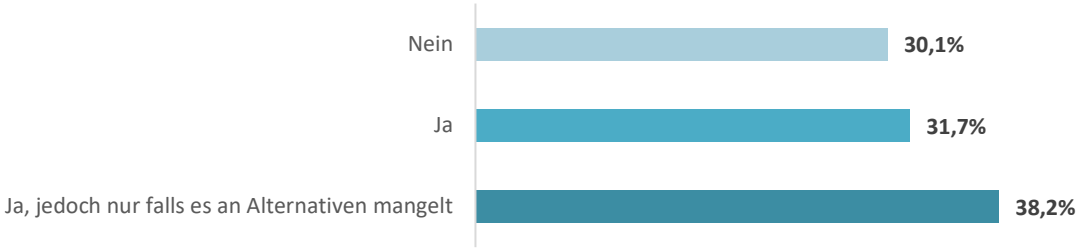


Abbildung 20: Nutzung trotz Fehlen der bevorzugten Authentifizierungsart

Identische Passwörter werden von 36,6 % der Befragten verwendet, wobei E-Commerce Plattformen, sensible und persönliche Daten und weniger relevante Webseiten nicht getrennt werden. 33,3 % gaben an, gleiche Passwörter nur für unbedenkliche Plattformen ohne E-Commerce Bezug zu verwenden. Die Minderheit von 30,1 % verwendet prinzipiell keine identischen Passwörter (vgl. Abbildung 21).

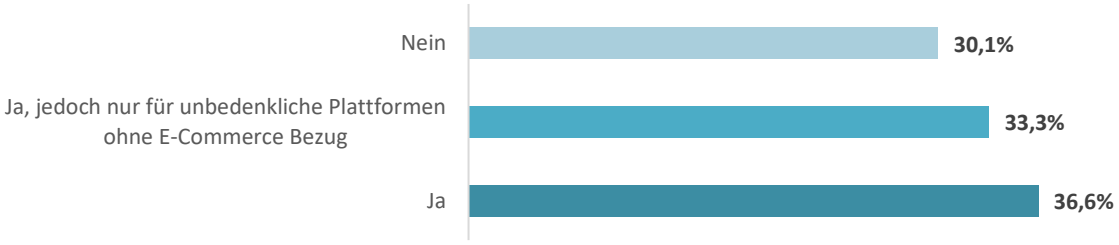


Abbildung 21: Nutzung identischer Passwörter

Die **Passwort-Mindestanforderungen** werden zwar von 49,6 % aller Befragten eingehalten, die jeweiligen Vorgaben jedoch nicht übertroffen. Eine Gruppe von 43,9 % gab an, die Mindestvorgaben zu übertreffen um höhere Sicherheit zu erlangen. Die Erhebung der Nutzung von identischen Passwörtern sowie den persönlichen Mindestanforderungen stellt die Grundlage für die Interpretation der darauffolgenden

Daten dieses Bereichs dar, und soll wertvolle Rückschlüsse auf das Nutzerverhalten und Sicherheitsbewusstsein geben.
Die Einschätzung der eigenen **Passwortstärke** kann der nachfolgenden Abbildung 22 entnommen werden.

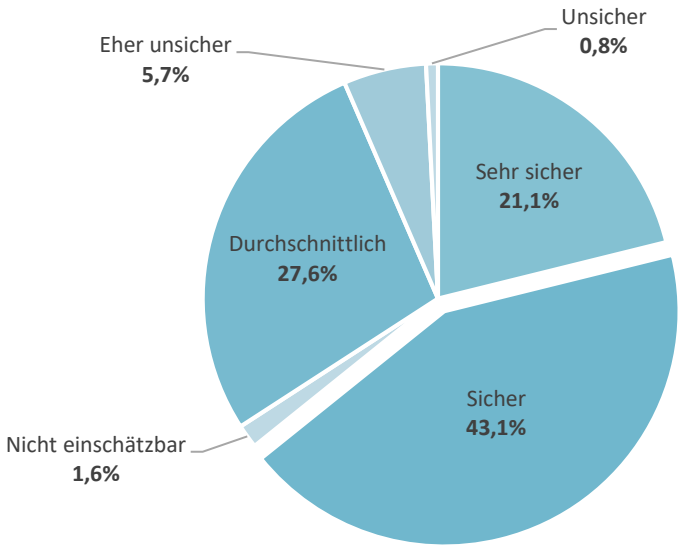


Abbildung 22: Einschätzung Passwortstärke

Obwohl von 49,6 % der Befragten lediglich die Mindestvorgaben eingehalten werden, gaben 43,1 % die eigene individuelle Passwortstärke als sicher, und zusätzliche 21,1 % der Befragten als sehr sicher an. Dadurch ergibt sich bereits ein gewisser Widerspruch, da ein Passwort mit einer vorgegebenen Stärke keinesfalls unter Garantie als sicher oder sogar sehr sicher bezeichnet werden kann. Diese Beobachtung deckt sich mit den Erkenntnissen aus Kapitel 4.4.3., wonach bei den Befragten ein hohes Selbstvertrauen erkennbar ist. Die Kreuztabelle ergibt, dass von 61 Teilnehmerinnen und Teilnehmern, welche sich an die Mindestvorgaben halten, diese jedoch nicht übertreffen, insgesamt 49,2 % ihr Passwort als sicher beziehungsweise sehr sicher einschätzen.
Um die tatsächliche Passwortsicherheit in Zusammenhang mit der subjektiven Wahrnehmung über Passwortsicherheit weiter zu erforschen, wurden Folgefragen nach unverzichtbaren Bestandteilen der verwendeten Passwörter, der Mindestanzahl an Zeichen sowie den jeweiligen Änderungsperioden gestellt.

Wie in Kapitel 3.2.1. ausgeführt, wird in der Literatur ein Basisschutz von mindestens acht Zeichen in Verbindung mit zumindest einem numerischen Wert, einem Sonderzeichen und der Verwendung von Groß- als auch Kleinbuchstaben angegeben. Lediglich 16,2 % der Befragten untertreffen die **Mindestlänge** von acht Zeichen. Ein kombinierter Anteil von 83,8 % erfüllt diese Anforderung, oder übertrifft diese sogar (vgl. Abbildung 23).

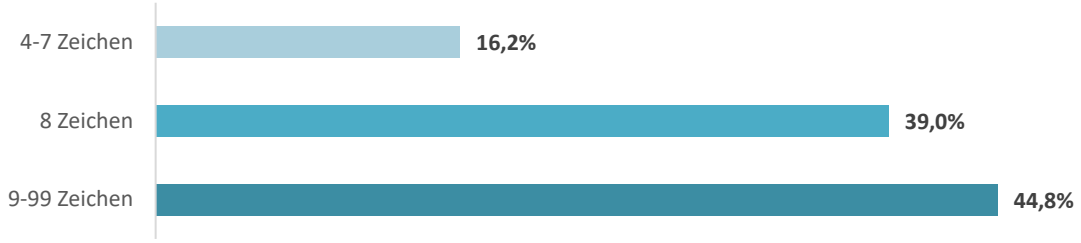


Abbildung 23: Passwortlänge Mindestanforderung

Ganz anders sieht es bei der Anforderung des Basisschutzes insgesamt aus. Hier können nur 28,5 % der Befragten eine zeitgemäße Passwortsicherheit durch Einhaltung aller Kriterien erlangen. Ganz klar zu beobachten ist hier eine Priorisierung auf die Anzahl der Zeichen, jedoch wird die tatsächliche **Zusammensetzung der Passwörter** selbst weitestgehend hintenangestellt. Wie im theoretischen Teil dieser Arbeit erwähnt, besitzt die Mindestlänge nur eine begrenzte Aussagekraft bezüglich der erzielbaren Sicherheit. Nur 56,1 % der Befragten gaben an, Sonderzeichen in ihren Passwörtern zu nutzen. Lediglich 28,5 % achten auf die Verwendung von Sonderzeichen oder numerischen Werten in der Passwortmitte.

Eine hohe Bereitschaft zur **Änderung der eigenen Passwörter** kann nicht festgestellt werden. Ein geringer Anteil von 23,6 % gab an, die Passwörter freiwillig und ohne zwingende Vorgabe der jeweiligen Plattform zu ändern. 39 % gaben an, die Passwörter unter keinen Umständen zu ändern während 37,4 % in Betracht ziehen, die Passwörter unter Vorgabe oder Zwang zu ändern (vgl. Abbildung 24).

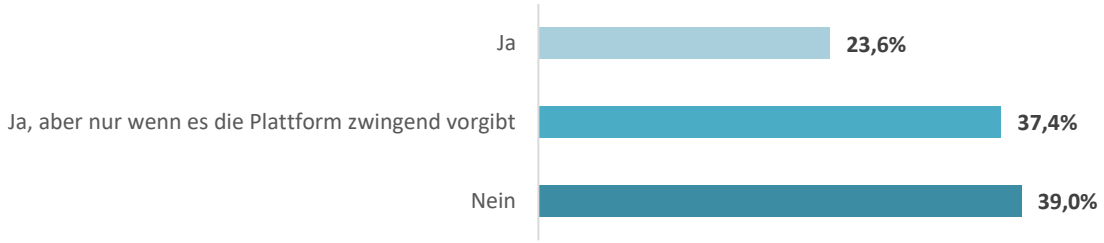


Abbildung 24: Regelmäßige Änderung eigener Passwörter

Die Diskrepanz zwischen subjektiver Wahrnehmung und tatsächlicher Sicherheitsstufe konnte durch die Abfrage von **Beispiel Passwörtern** näher bestimmt werden. Die abschließende Frage dieses Kapitels bot den Teilnehmenden eine Reihe von Passwörtern an, welche auf den ersten Blick sehr ähnlich, jedoch bezogen auf ihr Sicherheitslevel stark unterschiedlich ausfielen. Die Sicherheitsstufe wurde anhand eines Online Analysetools des Anbieters Cygnius ermittelt.[113]

Für die Fragestellung wurden verschiedene Passwörter unterschiedlicher Härte auserwählt und mittels einer Matrix abgefragt. Die Analyse ergab, wie bereits im Rahmen dieses Kapitels mehrmals vermutet, eine deutlich sichtbare Abweichung zwischen der subjektiv wahrgenommenen Stärke von Passwörtern und der objektiv bewerteten Sicherheitsstufe. So ergab ein relatives starkes Passwort, welches laut Analysetool 663 Jahre für ein erfolgreiches Knacken benötigen würde, ein Ergebnis von 54,5 % für die Zeiträume sofort, Minuten und Stunden. Dafür wurde einem scheinbar unsicheren Passwort von insgesamt 42,2 % der Teilnehmenden ein Zeitraum von Tagen über mehrere Wochen und Jahre bis hin zu Jahrzehnten zugerechnet.

[113] Cygnius Password Strength Test, URL: https://apps.cygnius.net/passtest (abgerufen am 14.12.2016)

Die genauen Ergebnisse dieser Analyse können der nachfolgenden Abbildung 25 entnommen werden. Neben dem Beispiel Passwort kann die errechnete theoretische Zeitspanne bis zu einem erfolgreichen Angriff abgelesen werden.

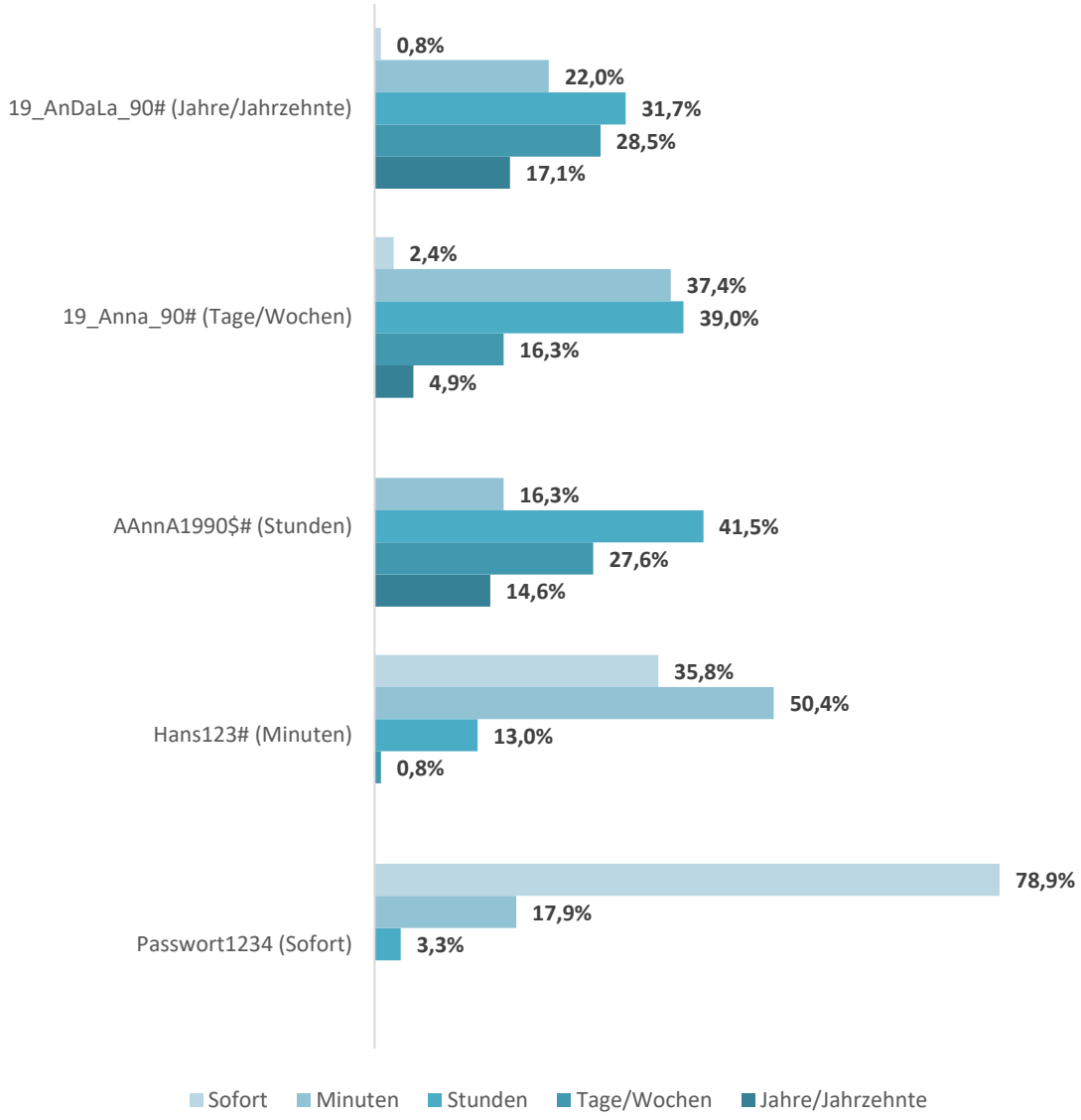


Abbildung 25: Beurteilung Beispiel Passwörter

Wie in der Auswertung gut sichtbar, wurden nur die relativ einfach erkennbaren Passwörter von der Mehrheit der Befragten richtig eingeordnet. Für die IT-Sicherheit relevant ist vor allem der Bereich von einigen Stunden bis hin zu Jahren. Oftmals ergibt sich nur ein kleines Zeitfenster für potentielle Angriffe, sodass ein Knacken von

komplexen Passwörtern wenig rentabel erscheint und damit auch weniger wahrscheinlich ist. Gerade in diesem Gebiet herrscht große Uneinigkeit zwischen den Teilnehmenden. So wird einem relativ sicheren Passwort mit nur 4,9 % eine deutlich niedrigere Sicherheitsstufe bescheinigt als einem Passwort, welches in wenigen Stunden erraten werden kann. Auch lässt sich kein Unterschied feststellen zwischen dem Passwort der höchsten Stufe und einem Passwort mittlerer Sicherheit unter einer zu erwartenden Zeitspanne von 11 Stunden. Hier herrscht deutlicher Aufklärungsbedarf, vor allem bezüglich der noch immer weit verbreiteten Meinung, die Anzahl der Zeichen wäre ein zuverlässiger Indikator für die Passwortsicherheit.

4.4.5. Session Management

Die Verwendung einer sicheren Verbindung bildet die Grundlage für eine sichere Verwendung der zahlreichen E-Commerce Plattformen. Diverse Browser und Technologien bieten auf diesem Gebiet zahlreiche Hilfestellungen für die Nutzerinnen und Nutzer an (vgl. Kapitel 3.3.).

Die eingehende Frage dieses Bereichs lautet daher, ob generell auf eine **sichere Verbindung** geachtet wird. In weiterer Folge ist zu klären, ob eine Awareness über die potentiellen Folgen einer unsicheren Session beziehungsweise Verbindung feststellbar ist.

Mit 48,8 % achtet knapp die Hälfte aller Befragten auf eine HTTPS Verbindung, welche gleichzeitig die einfachste Möglichkeit darstellt, eine sichere Verbindung zu nutzen (vgl. Abbildung 26).

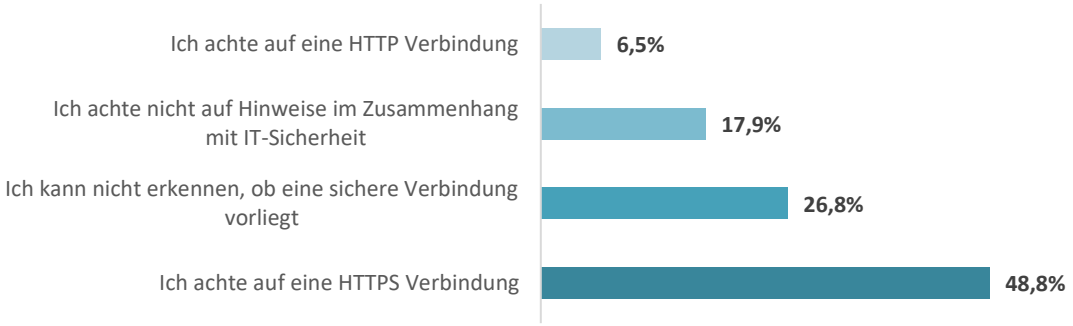


Abbildung 26: Überprüfung Verbindungsart

Für die real erzielbare Sicherheit ist dieser Wert dennoch als sehr gering anzusehen, da zunächst die kombinierte Mehrheit von 51,2 % HTTPS nicht nutzen beziehungsweise nicht selbst erkennen können, welche Verbindungsart genutzt wird. Die Folgefrage bezüglich der **Überprüfung von HTTPS** zeigt weitere Diskrepanzen zwischen dem Nutzerverhalten und der erzielbaren Sicherheitsstufe. So gaben jene 60 Befragte an, welche auf den Zusatz HTTPS Wert legen, nur in 15 % der Fälle über den Browser auf Detailinformationen der Verbindung zu achten. Die für die tatsächliche Sicherheit wenig ausschlaggebenden Merkmale wie der Zusatz HTTPS in der Adresszeile des Browsers oder ein grünes Symbol wurden von 81,7 % beziehungsweise 61,7 % angegeben. 15 % gaben an, keine weiteren Überprüfungen durchzuführen (vgl. Abbildung 27).

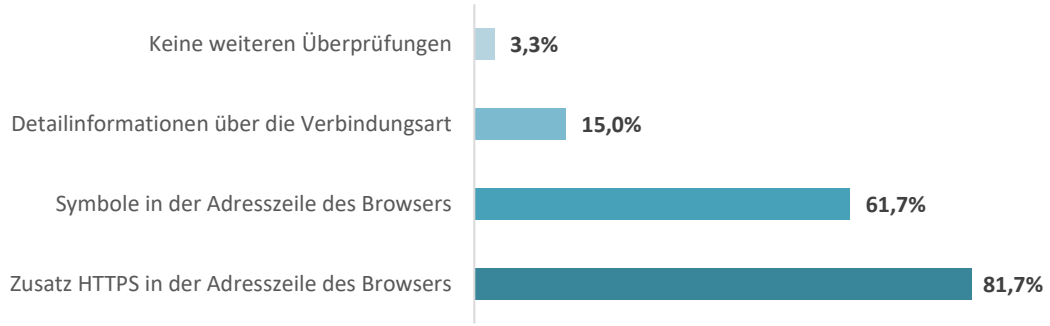


Abbildung 27: Überprüfung HTTPS

Bezüglich der Frage nach der Möglichkeit eines Session Hijackings, also der **Übernahme einer eigenständigen Session** inklusive den persönlichen Daten sowie einem allfälligen Warenkorb sowie den Zugangsdaten selbst, konnten nur 29,3 % der Befragten angeben, sich davor schützen zu können. Der verbleibende Teil von insgesamt 70,7 % kannte das Risiko entweder nicht (12,2 %), legte keinen Wert darauf (13 %) oder wusste nicht welche Schutzmaßnahmen für diesen Fall existieren (45,5 %). Dieser Umstand ist bedenklich, da anscheinend die Information selbst zu einem sehr großen Anteil vorhanden ist, jedoch dennoch ein großer Anteil keine Möglichkeit sieht, sich davor zu schützen (vgl. Abbildung 28).

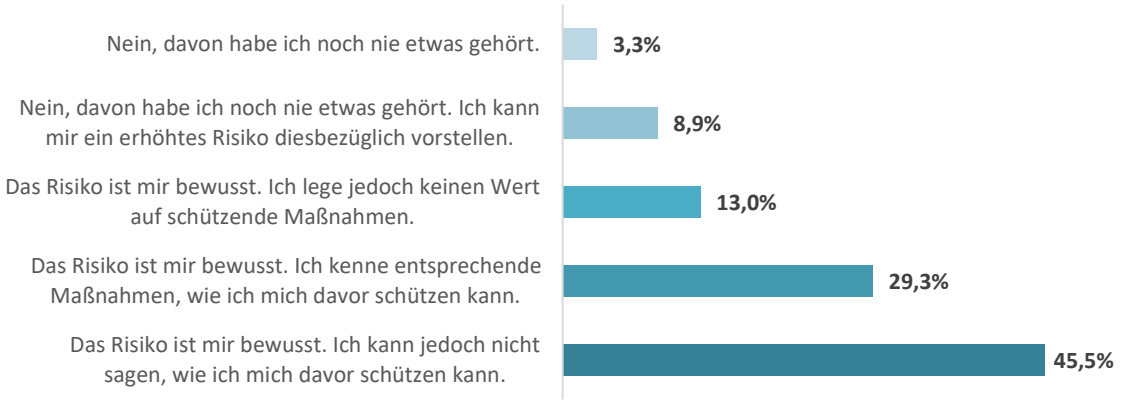


Abbildung 28: Einschätzung Gefahrenpotential Session Hijacking

Um das Nutzerverhalten im Bereich Session Management noch genauer zu erforschen, wurde zusätzlich die **Kenntnis über die Funktionsweise von Zertifikaten** und deren Bedeutung für die Sicherheit einer E-Commerce Plattform erhoben.

Abbildung 29 zeigt die Auswertung der Frage nach der Funktionsweise und dem Umgang mit Zertifikaten.

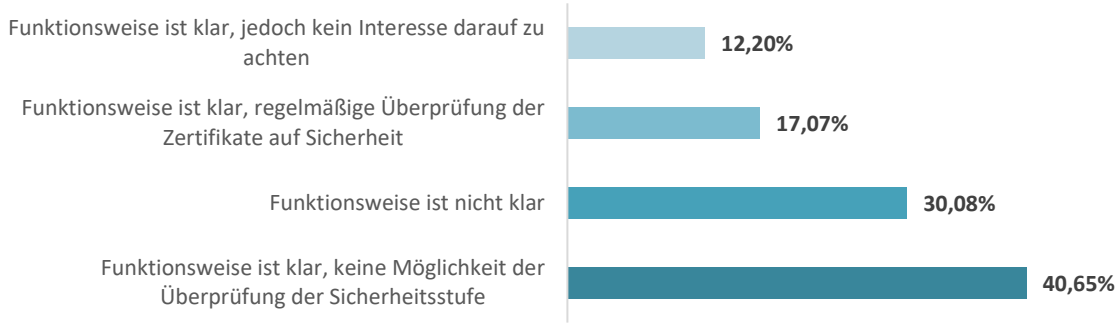


Abbildung 29: Umgang mit Zertifikaten

Wie in Kapitel 3.5. erläutert, stellen Zertifikate ein wichtiges Mittel dar, um E-Commerce Transaktionen sicher abzuwickeln. Ein kumulierter Anteil von 82,89 % der Befragten hat entweder kein Interesse an der Überprüfung, die Funktionsweise ist nicht klar oder es fehlt das entsprechende Wissen um die Zertifikate zu überprüfen. Auch hier zeigt sich fehlendes Hintergrundwissen, um mit den vorhandenen Tools und Methoden zielführend umgehen zu können. Ein geringer Anteil von 17,07 % überprüft Zertifikate auf deren Gültigkeit und Sicherheitsstufe.

4.4.6. Cookies

Cookies entsprechen einem unverzichtbaren Bestandteil jeder Browser Session sowie üblicher E-Commerce Transaktionen. Wie in Kapitel 3.4. beschrieben, beinhalten Cookies zwar ein gewisses Angriffspotential, jedoch führt die Deaktivierung von Cookies zu einer noch viel größeren Angriffsfläche und damit zu einem erhöhten Sicherheitsrisiko. Im Rahmen der Erhebung wurde gezielt nach der Verwendung von Cookies gefragt, sowie Folgefragen zu der kategorischen Ablehnung gestellt, welche von vielen E-Commerce Nutzern als Lösung für Sicherheitsbedenken angesehen wird.

Die Verteilung bezüglich der **Nutzung und Überprüfung von Cookies** lässt sich aus der nachfolgenden Abbildung 30 ablesen.

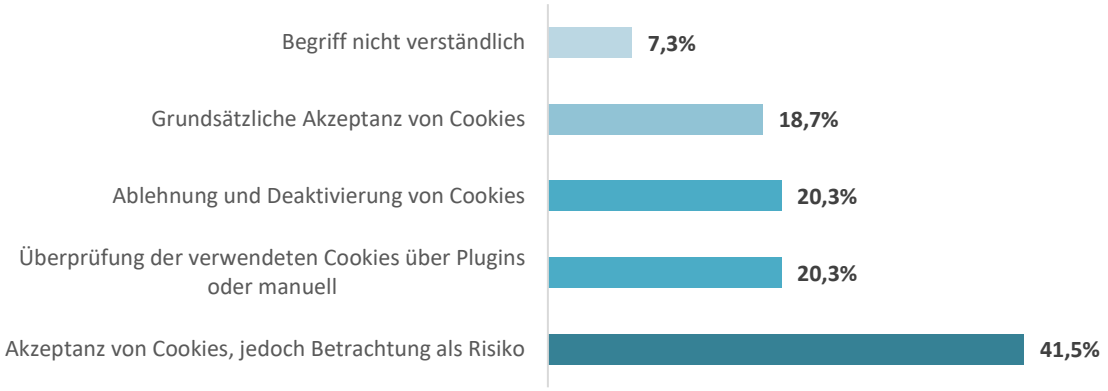


Abbildung 30: Verwendung von Cookies

Ein Anteil von 41,5 % der Befragten akzeptiert die Verwendung von Cookies, sieht diese aber als Risikofaktor an. Weitere 20,3 % deaktivieren Cookies und lehnen diese kategorisch ab. Ein Anteil von 20,3 % überprüft das Sicherheitslevel der verwendeten Cookies manuell oder über Browser Plugins. Als **Gründe für eine mögliche Ablehnung** wurde von insgesamt 23 Befragten, welche Cookies grundsätzlich akzeptieren, im Ausmaß von 60,9 % Sicherheitsbedenken angegeben. Ein Anteil von 69,6 % sieht den Datenschutz durch die Verwendung von Cookies gefährdet (vgl. Abbildung 31).

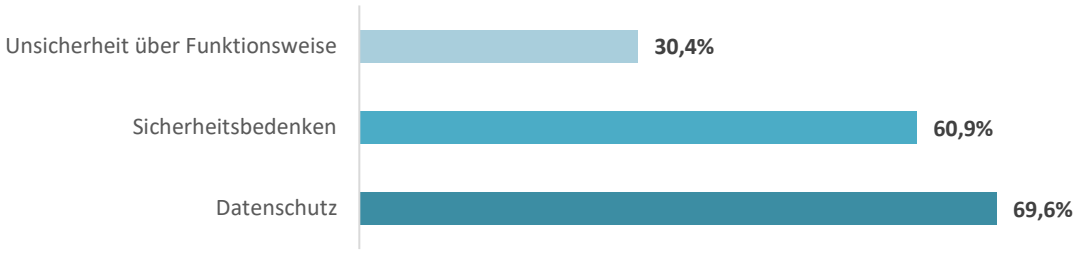


Abbildung 31: Gründe für eine mögliche Ablehnung von Cookies

Hier zeigen sich enorme Defizite in Bezug auf das Grundverständnis von IT-Sicherheit im E-Commerce. Die Deaktivierung von Cookies stellt keine Erhöhung der Sicherheit

dar, zusätzlich sollte bei Verwendung von Cookies stets deren Status und Gültigkeit überprüft werden.

Zu der Frage nach dem **An- und Abmeldeverhalten** gaben 48 % an, sich stets manuell abzumelden, sobald eine Webseite verlassen wird. Ein Anteil von 28,3 % gab an, auf die Zeitperiode bis zu einer allfälligen automatischen Abmeldung zu achten. Lediglich 13 % der Befragten wählen die Option der dauerhaften Anmeldung, der geringe Anteil von 9,8 % bevorzugt eine Anmeldung auch über den Neustart des Endgerätes hinaus. Diese Zahlen sprechen für eine hohe Awareness der Teilnehmenden bezüglich Cookies.

4.4.7. Browser Erweiterungen

Browser Erweiterungen bieten eine Erleichterung in vielen Aspekten der täglichen Internet Nutzung und sind ein unverzichtbarer Bestandteil von vielen E-Commerce Portalen und Webseiten. Dies bestätigen 89,4 % der Befragten, welche die **Nutzung von Browser Erweiterungen** beziehungsweise Funktionalitäten angaben. Veraltete und aus IT-Sicherheit bedenkliche Plugins wie ActiveX nutzen lediglich 12,2 % der Teilnehmerinnen und Teilnehmer. Meistverbreitete Plugins wie Adobe Flash oder Java finden zu je 52 % und 35,8 % Anwendung. Die automatische Speicherung von Passwörtern oder Formulardaten wird von 39 % beziehungsweise 33,3 % genutzt (vgl. Abbildung 32). Die Nutzung von sonstigen Plugins wurde nur von drei Befragten angegeben.

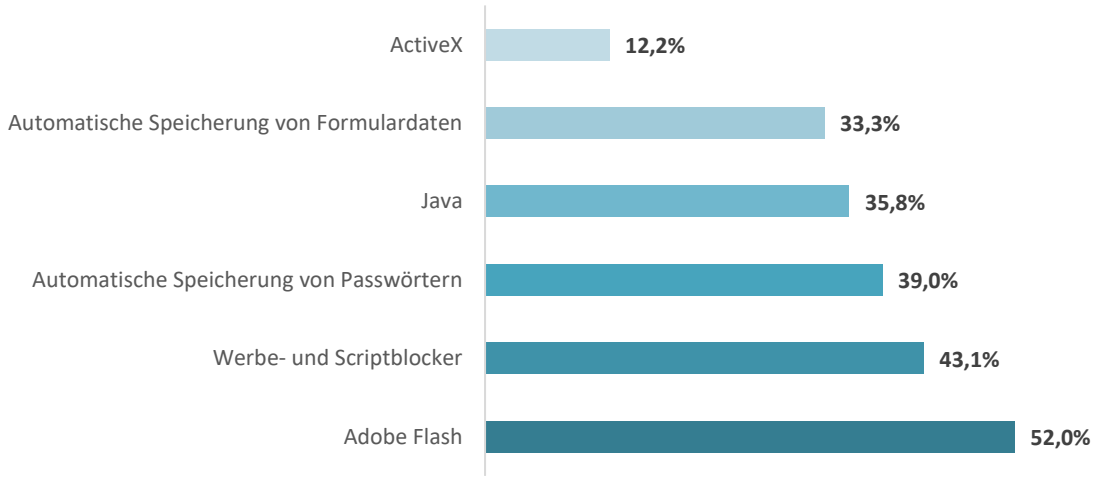


Abbildung 32: Nutzung von Browser Erweiterungen

Wie in Kapitel 3.6. ausgeführt, stellt die automatische Speicherung von sensiblen Daten ein erhöhtes Sicherheitsrisiko dar. Dennoch nutzen mehr als ein Drittel aller Befragten diese Funktionalität. Auch die Verwendung von Adobe Flash lässt Defizite im Sicherheitsbewusstsein der Befragten vermuten, zumal bereits Alternativen im Bereich der Browser Technologien und Webseiten existieren. Positiv hervorzuheben ist die Nutzung von Plugins, welche Werbung, Skripte oder ähnliches blockieren. Diese Art von Funktionalität wird von 43,1 % der Teilnehmerinnen und Teilnehmer genutzt.

4.4.8. Gütesiegel

Gütesiegel sind ein wichtiger Indikator für die Sicherheit einer E-Commerce Plattform, jedoch nur unter ausreichender Überprüfung der Echtheit des jeweiligen Siegels. Erforscht wurde zunächst, welche **Gütesiegel** unter den Befragten bekannt sind sowie in weiterer Folge, wie und ob die **Gültigkeit** beziehungsweise **Echtheit** eines solchen Siegels seitens der Nutzer überprüft wird.

Der angegebene Stellenwert kann der nachfolgenden Abbildung 33 entnommen werden.

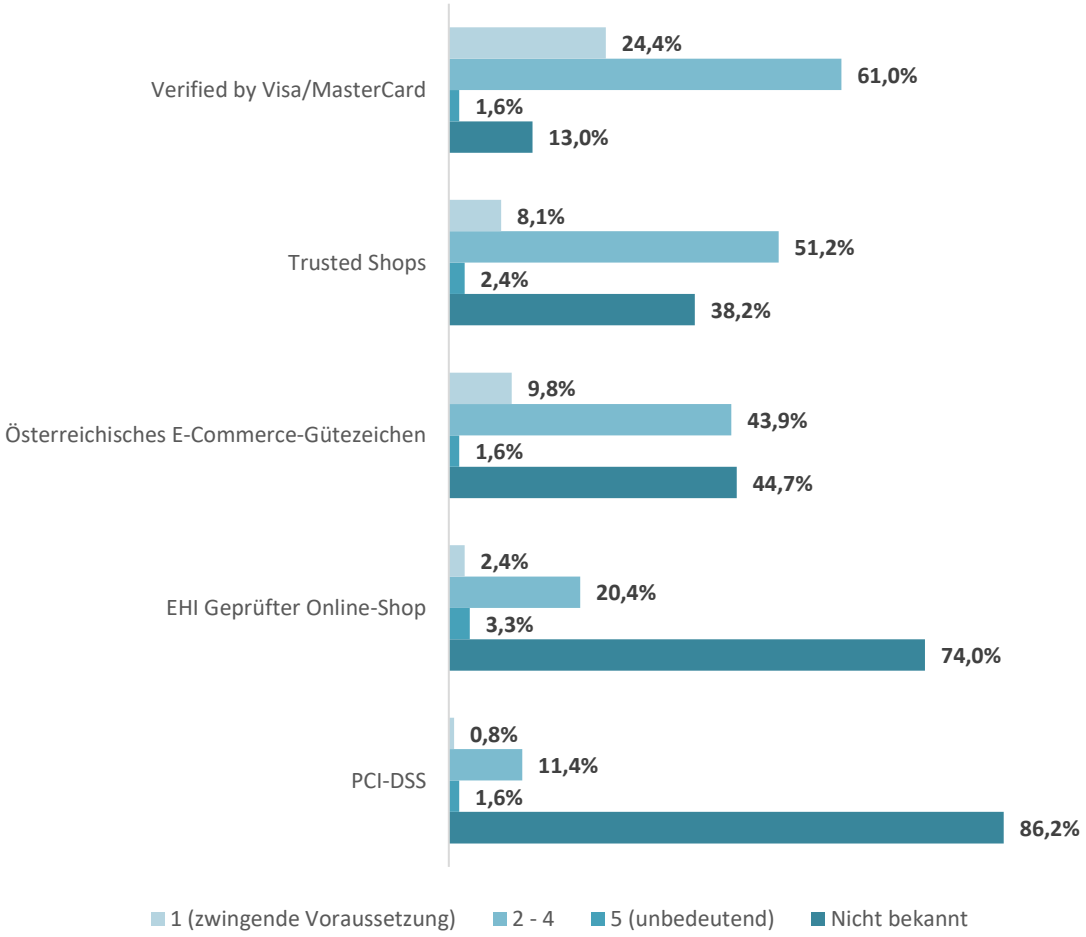


Abbildung 33: Stellenwert von Gütesiegeln

Die für eine sehr hohe Sicherheit einstehenden Standards wie beispielsweise PCI-DSS (vgl. Kapitel 3.7.1.) ist einem Großteil der Befragten weitestgehend unbekannt. Bekannt ist dagegen Verified by Visa/MasterCard, auf dieses Gütesiegel wird von 85,4 % geachtet, 24,4 % betrachten es sogar als zwingende Voraussetzung. Wie in der Auswertung der Folgefrage ersichtlich ist, legen 35 % der Teilnehmerinnen und Teilnehmer keinen Wert auf Gütesiegel, und achten auch nicht darauf (vgl. Abbildung 34). Dieser Umstand ist bedauerlich, da hiermit die verschiedenen Netzwerke und Security Audits, durch welche sich E-Commerce Plattformen in Bezug auf die IT-Sicherheit unterscheiden, nur wenig Relevanz besitzen.

Die Teilnehmerinnen und Teilnehmer dieser Studie sollten im Rahmen der Folgefrage beantworten, ob auch die **Echtheit des Siegels** überprüft wird. Ohne weitere Überprüfung besitzt das reine Vorhandensein eines Siegels keine Aussagekraft (vgl. Abbildung 34).

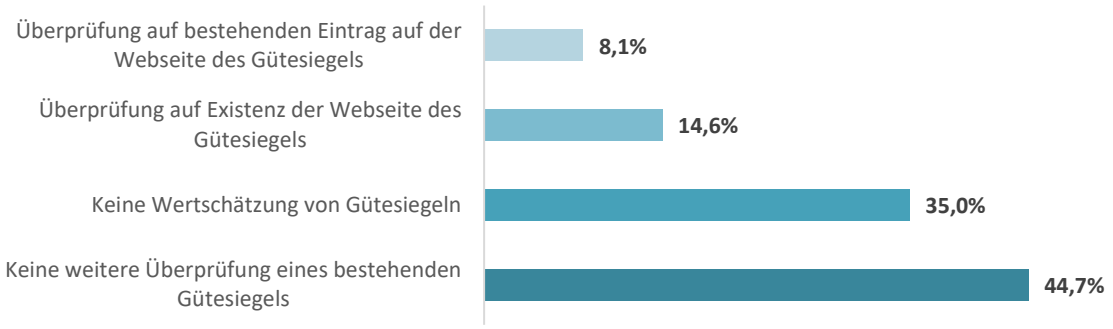


Abbildung 34: Überprüfung von Gütesiegeln

Dieses Ergebnis stellt einen Rückschlag für die Entwicklung und zumeist kostenintensive Auditierung vieler E-Commerce Plattformen dar. Der sehr geringe Prozentsatz von nur 8,1 % überprüft die Echtheit eines Gütesiegels auf der jeweiligen Anbieterplattform. Die Überprüfung der Existenz eines Gütesiegels, welches von 14,6 % der Befragten angegeben wurde, kann bezüglich der potentiellen IT-Sicherheitsstufe zur Gänze ignoriert werden. Zu einfach ist es, ein Logo oder einen Schriftzug schlichtweg zu fälschen.

4.5. Fazit der Erhebung

Die Auswertung der Studie zeigt zunächst großen Aufholbedarf in verschiedenen Bereichen der IT-Sicherheit in Verbindung mit E-Commerce Plattformen. Als Ausgangsbasis der individuellen Nutzerwahrnehmung konnten zu einem Großteil Motive der Bequemlichkeit und produktspezifische Besonderheiten erkannt werden. Bedenken bezüglich unzureichender Sicherheit oder die Angst vor finanziellem Schaden und einer unsicheren Verbindung wurde nur von einer Minderheit der Befragten bestätigt. Die Risikowahrnehmung stellt die Grundlage für eine bewusste Awareness bezüglich IT-Sicherheit dar. Erschwerend hinzu kommt die Tatsache, dass hauptsächlich sicherheitstechnisch sensible Transaktionsverfahren wie beispielsweise die Kreditkarte

oder die Plattform PayPal genutzt werden. Auch hier zeigt sich unzureichende Aufmerksamkeit bezüglich der zur Verfügung stehenden Optionen, da selbst das Fehlen eines TAN/Secure Code Verfahrens für mehr als zwei Drittel der Befragten keinen Abbruchgrund darstellt.

Im Bereich der Authentifizierung konnte beobachtet werden, dass es eine hohe Diskrepanz zwischen der tatsächlichen und der subjektiv wahrgenommenen Passwortsicherheit gibt. Die Einschätzung der eigenen Passwortsicherheit widerspricht der fehlenden Bereitschaft, Passwörter regelmäßig zu ändern sowie auch der nur unzureichend korrekten Einschätzung der Passwortstärke von angegebenen Beispielen. Auch mittlerweile vielseitig kommunizierte Fakten, wie beispielsweise die geringe Relevanz der Passwortlänge an sich, konnten aus den erhobenen Daten nicht abgelesen werden. Hier ist bereits erkennbar, dass es zu einer immer größer werdenden Lücke zwischen den aktuellen IT-Sicherheitsbedrohungen und der Nutzerwahrnehmung kommt.

Die Überprüfung einer sicheren Verbindung wurde von rund der Hälfte aller Befragten angegeben. Dieser Wert liegt unter den Erwartungen, und wird durch die Auswertung der Folgefrage nach der Methodik der Kontrolle einer sicheren Verbindung weiter beeinträchtigt. Lediglich ein sehr geringer Prozentsatz nutzt die Möglichkeit, Detailinformationen über die Verbindungsart abzurufen, was einem immer noch vorhandenen Sicherheitsrisiko entspricht. Die Mehrheit verlässt sich auf einfache Symbole oder den Zusatz HTTPS in der Adresszeile des Browsers. Die Echtheit von Zertifikaten wird von weniger als einem Fünftel der Befragten regelmäßig überprüft. Dem Großteil der Teilnehmerinnen und Teilnehmer ist die Funktionsweise nicht klar, oder es gibt Unklarheiten über die Möglichkeiten der Überprüfung.

Zu dem Thema Cookies zeigt sich hohe Unwissenheit und Fehlinterpretation der Funktionsweise dieser Technologie. Cookies werden demnach weitestgehend akzeptiert, jedoch überprüft nur ein geringer Prozentsatz die Detailinformationen über Browser Plugins oder manuell. Starke Defizite im tatsächlichen Nutzerverhalten zeigt der hohe Anteil von Befragten, welche Cookies grundsätzlich deaktivieren um die Sicherheit zu erhöhen. Dies entspricht allerdings einem erhöhten Sicherheitsrisiko, da die Session Abwicklung einer E-Commerce Webseite, ohne die Verwendung von Cookies zuzulassen, ein umso höheres Gefahren- und Angriffspotential darstellt.

Der bisher gewonnene Eindruck über die Nutzerwahrnehmung und das daraus resultierende Verhalten in Bezug auf E-Commerce konnte auch durch die Auswertung zu den Themen Browser Erweiterungen und Gütesiegel bestätigt werden. So werden sensible Browser Erweiterungen von rund einem bis zwei Drittel der Befragten genutzt. Veraltete Plugins wie beispielsweise ActiveX werden dahingegen nur von einem geringen Prozentsatz verwendet. Gütesiegel, welche einen aussagekräftigen Indikator für die Sicherheitsstufe im Allgemeinen, aber auch die im Hintergrund befindliche IT-Architektur im Speziellen darstellen, werden von den Befragten weitestgehend ignoriert. Selbst bei Beachtung kommt es nur bei einem sehr geringen Anteil der Teilnehmerinnen und Teilnehmer zu einer weiteren Überprüfung.

Zusammenfassend kann festgestellt werden, dass die Auswertung dieser Studie eine klare Bestätigung der dieser Arbeit zugrundeliegenden Hypothese zeigt, wonach trotz laufender Verbesserung und Weiterentwicklung im Bereich der IT-Sicherheit, die Auswirkungen auf das tatsächliche Nutzerverhalten nur als gering anzusehen sind. Gründe hierfür wurden im Rahmen dieser Arbeit nicht erforscht und entsprechen einem möglichen Forschungsgegenstand für zukünftige Thesen.

5. Conclusio

Im diesem abschließenden Kapitel soll eine Zusammenfassung über die Beantwortung der Forschungsfrage, die Prüfung der Hypothese sowie ein Überblick über die grundlegenden Bestandteile dieser Arbeit gegeben werden. Ein Ausblick auf die Zukunft schließt dieses Kapitel und damit auch diese Masterthesis ab.

5.1. Forschungsergebnis

Im Rahmen dieser Arbeit sollte die Forschungsfrage beantwortet werden, inwiefern IT-Sicherheit das Nutzerverhalten von Konsumierenden im Rahmen des E-Commerce beeinflusst. Hierfür wurde eine Hypothese aufgestellt, nach welcher die tatsächlichen Auswirkungen auf das Nutzerverhalten unter einer laufenden und stetigen Weiterentwicklung auf dem Gebiet der IT-Sicherheit, nur als sehr gering anzusehen sind.

Nach einer ausführlichen Literaturrecherche auf dem Gebiet der IT-Sicherheit im Bereich des E-Commerce, aktueller Bedrohungen und der Definition der Schutzziele wurde im ersten Teil dieser Arbeit auf E-Commerce als Geschäftsmodell und dessen Nutzenpotentiale für Anbieter und Konsumierende eingegangen. Nachteile und Risiken wurden im Zuge der Recherche ebenfalls erhoben. Ergänzt und vervollständigt wurde das Kapitel von der Vorstellung vorhandener und genutzter Zahlungssysteme.
Im zweiten Themenbereich des theoretischen Teils dieser Arbeit konnten Risiken im E-Commerce erhoben und bewertet werden. Es erfolgte eine Unterteilung in die Überbegriffe Authentifizierung, Session Management, Cookies, Zertifikate sowie Browser Erweiterungen und Gütesiegel. Der aktuelle Stand der Technik wurde vorgestellt und Best Practice Ansätze erörtert

Im empirischen Teil dieser Arbeit sollte die Frage beantwortet werden, welchen Einfluss die IT-Sicherheit auf das Nutzerverhalten von Konsumenten im E-Commerce ausübt. Die Hypothese dieser Arbeit, welche nur geringe Auswirkungen auf das reale Nutzerverhalten unterstellte, sollte durch eine quantitative Online-Erhebung mittels Selbstselektion bestätigt oder verworfen werden. Das Ergebnis dieser Studie ist nicht

repräsentativ für die Grundgesamtheit, wie in Kapitel 4.2.4. näher erläutert. Vielmehr entspricht es einem Trend, welcher Hinweise auf die grundsätzliche Ausrichtung der Zielgruppe gibt.

Nach Auswertung der erhobenen Daten kann im Zuge der Datenanalyse eine Bestätigung der Hypothese erzielt werden. Der technische Fortschritt steht unvermeidbar raffinierten und ebenfalls stetig weiterentwickelten Angriffsmethoden gegenüber. Methoden auf der Nutzerseite, welche solche Angriffe erkennen und verhindern lassen, sind mit einfachen Mitteln nicht zu realisieren. Browser Plugins und Technologien bieten zwar grundsätzlich Tools an, um den Nutzern eine Überprüfung der zahlreichen Systeme zu ermöglichen, der Wissensstand eines Großteils der Befragten lässt jedoch auf teils veraltete oder unzureichende Kenntnisse schließen. Zu einfach und unzuverlässig sind die direkten Methoden wie beispielsweise Symbole in der Browser Adresszeile oder die reine Abbildung eines Gütesiegels auf einer E-Commerce Plattform, zu komplex, wenig transparent und nicht nachvollziehbar die sicheren und zuverlässigen Methoden.
Daraus ergibt sich ein unvermeidbarer Spalt zwischen der subjektiven Wahrnehmung von IT-Sicherheit im E-Commerce und der Realität. Die Tatsache, dass viele Methoden zahlreiche zusätzliche Schritte und Klicks erfordern, lässt sich aus den gewonnen Daten als weitere Hürde auf dem Weg zu sicheren Transaktionen ablesen. Die Datenanalyse zeigt in den meisten Fällen eine niedrige Bereitschaft, diese zusätzlichen Schritte auszuführen, unabhängig von Kenntnis und Risikowahrnehmung.
Die Lösung dieses Problems erfordert eine umfangreiche Forschung auf dem Gebiet der Nutzerwahrnehmung und Einschätzung von aktuellen IT-Sicherheitsrisiken. Im nachfolgenden Kapitel sollen im Rahmen eines Forschungsausblicks Ansätze gefunden werden, diesen Zustand nachhaltig zu verbessern.

5.2. Forschungsausblick

Die in dieser Arbeit erforschten Defizite und Fehleinschätzung seitens der Konsumierenden stellen einen zentralen Bestandteil zukünftiger Forschungen dar. Ein weiterer Ansatz liegt in der Verbesserung der verfügbaren Online Tools und Technologien, um dem Nutzer das Leben zu vereinfachen. So macht es nur wenig Sinn,

die Technologien welche ein Browser nicht zur Gänze autonom und zuverlässig erkennen kann, immer weiter zu verbessern. Beide Themen gleichzeitig weiterzuentwickeln kann ein probates Mittel für eine Erhöhung der IT-Sicherheit im Bereich des E-Commerce darstellen, die Konzentration auf eines dieser Themen könnte jedoch schneller und effizienter zum Ziel führen. Hier gibt es zahlreiche Forschungsansätze, welche sowohl auf das Nutzerverhalten als auch auf die Wahrnehmung von Technologien und Sicherheitsfunktionalitäten abzielen.

Der erste Forschungsbereich liegt in der Konzentration auf die E-Commerce Nutzer selbst. Aufklärungsarbeit, Transport von Wissen oder elektronische Lernportale sind nur einige Möglichkeiten, Interesse zu wecken. Die Kosten hierfür könnten von der Wirtschaft getragen werden, ähnlich wie bei vergleichbaren Initiativen in der Vergangenheit. Hierzu wären Studien sinnvoll, die ganz gezielt auf das Nutzerverhalten und die Wahrnehmung ausgerichtet sind. Die Alternative liegt im besseren und vollautomatisierten Handling von Sicherheitstechnologien. Hierbei könnte das Forschungsziel lauten, den Nutzer weitestgehend zu ignorieren und dabei gleichzeitig eine höhere Sicherheit zu erzielen, ohne dessen aktive Mitarbeit. Die Erfahrung zeigt jedoch eine hohe Kreativität der Angreifer, wodurch selbst die neuesten Technologien und Systeme ausgehebelt werden könnten. Trotzdem ist es denkbar, neuartige Programme und Methoden zu entwickeln, mit welchen der Nutzer vor sich selbst geschützt werden kann, in einer zuverlässigen Form und unter einem geringen Sicherheitsrisiko.

Beide vorgestellten Forschungsbereiche sind aus der Sicht des Verfassers dieser Arbeit denkbar und zielführend, wobei die Konzentration auf die Erforschung der Wahrnehmung und dessen gezielte Beeinflussung eine nachhaltigere Variante darstellen sollte.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bücher

Aichele, Christian; Schönberger, Marius: E-Business: Eine Übersicht für erfolgreiches B2B und B2C, Springer: Wiesbaden, 2016

Beissel, Stefan: Cybersecurity Investments: Decision Support Under Economic Aspects, Springer: International Publishing Switzerland, 2016

Braunecker, Claus: How to do Empirie, how to do SPSS: Eine Gebrauchsanleitung, UTB: Stuttgart, 2016

Heinemann**,** Gerrit: Der neue Online-Handel: Geschäftsmodell und Kanalexzellenz im Digital Commerce, 7. Aufl., Springer: Wiesbaden, 2016

Hug Theo; Poscheschnik, Gerald: Empirisch forschen, 2. Aufl., UTB: Stuttgart, 2014

Klipper, Sebastian: Cyber Security: Ein Einblick für Wirtschaftswissenschaftler, Springer: Wiesbaden, 2015

Kuckartz, Udo; Ebert, Thomas; Rädiker, Stefan; Stefer, Claus: Evaluation online: Internetgestützte Befragung in der Praxis, VS Verlag für Sozialwissenschaften: Wiesbaden, 2009

Lepofsky, Ron: The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web, Apress: New York, 2012

Olbrich, Rainer; Schultz, Carsten D.; Holsing, Christian: Electronic Commerce und Online-Marketing: Ein einführendes Lehr- und Übungsbuch, Springer: Berlin Heidelberg, 2015

Raab-Steiner, Elisabeth; Benesch, Michael: Der Fragebogen: Von der Forschungsidee zur SPSS-Auswertung, 4. Aufl., UTB: Stuttgart, 2015

Rohr, Matthias: Sicherheit von Webanwendungen in der Praxis: Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse, Springer: Wiesbaden, 2015

Stahl, Ernst; Wittmann Georg, Krabichler, Thomas; Breitschaft, Markus: E-Commerce-Leitfaden, 3. Aufl., Universitätsverlag Regensburg: Regensburg, 2012

Stallmann, Franziska; Wegner, Ullrich: Internationalisierung von E-Commerce-Geschäften: Bausteine, Strategien, Umsetzung, Springer: Wiesbaden, 2015

Wirtz, Bernd W..: Electronic Business, 4. Aufl., Springer: Wiesbaden, 2013

Zeitschriften

Ackermann, Tobias; Bedner, Mark: Schutzziele der IT-Sicherheit, in: Datenschutz und Datensicherheit 2010, Ausgabe 5

Internet

Cygnius Password Strength Test, URL: htps://apps.cygnius.net/passtest (abgerufen am 14.12.2016), Cygnius Network Resource Centre, 2006-2017

Das große Online-Lexikon für Informationstechnologie, URL: http://www.itwissen.info/definition/lexikon/IT-Sicherheit-IT-security.html (abgerufen am 14.12.2016), DATACOM Buchverlag GmbH, Peterskirchen, 2016

Enzyklopädie der Wirtschaftsinformatik, URL: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html (abgerufen am 14.12.2016), Universität Potsdam, Potsdam, 2016

Statista: Prognose zur Anzahl der E-Commerce-Nutzer weltweit in den Jahren 2015 bis 2021 (in Millionen), URL: https://de.statista.com/statistik/daten/studie/485005/umfrage/prognose-der-e-commerce-nutzer-weltweit (abgerufen am 14.12.2016), Statista Digital Market Outlook, 2016

Trusted Shops Gütesiegel: Die Qualitätskriterien von Trusted Shops, URL: http://www.trustedshops.at/guetesiegel/einzelkriterien.html (abgerufen am 14.12.2016), Trusted Shops GmbH, Köln, 2016

FERDINAND PORSCHE
FERN FH

0% ausgefüllt

Sehr geehrte Teilnehmerinnen und Teilnehmer,

Im Zuge meiner Masterarbeit im Studiengang "Wirtschaftsinformatik" an der Ferdinand Porsche FernFH führe ich eine Befragung zur Erforschung des

Einflusses der IT-Sicherheit im Bereich des E-Commerce auf das Nutzerverhalten von Konsumenten durch.

Ich möchte mich für Ihr Interesse und Ihre Teilnahme an meiner Umfrage ganz herzlich bedanken.

Die Umfrage umfasst je nach Auswahl ca. 30 Fragen und nimmt ca. **5-10 Minuten** Ihrer Zeit in Anspruch. Alle Daten werden **vertraulich** und **anonymisiert** behandelt und nicht an Dritte weitergegeben. Sie dienen ausschließlich wissenschaftlichen Zwecken.

Gerne können Sie den Link zu diesem Online-Fragebogen an Freunde, Bekannte und Kollegen weiterleiten. Durch zusätzliche Teilnehmerinnen und Teilnehmer wird die Aussagekraft dieser Studie weiter erhöht.

Sollten Sie Fragen zur Umfrage oder zu dem Thema selbst haben, stehe ich Ihnen sehr gerne unter der E-Mail Adresse thomas.trillsam@mail.fernfh.ac.at zur Verfügung.

Vielen Dank im Voraus für Ihre Unterstützung,

Thomas Trillsam, BSc

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

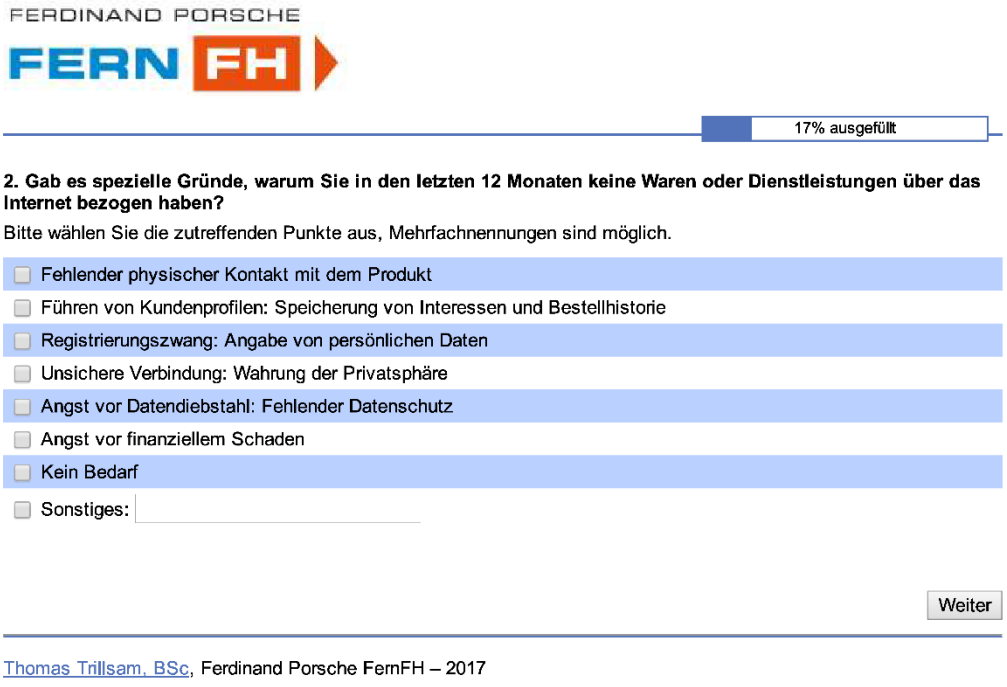
8% ausgefüllt

1. Wie häufig haben Sie das Internet innerhalb der letzten 12 Monate für den Kauf von Gütern oder Dienstleistungen genutzt?

- ○ Regelmäßig, mehrmals pro Woche
- ○ Regelmäßig, mehrmals pro Monat
- ○ Unregelmäßig, aber zumindest in Intervallen von jeweils 6 – 8 Wochen
- ○ Unregelmäßig, nur einzelne Transaktionen über das gesamte Jahr verteilt
- ○ Ich habe in den letzten 12 Monaten keine E-Commerce Transaktionen vorgenommen

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017


FERDINAND PORSCHE
FERN FH

17% ausgefüllt

2. Gab es spezielle Gründe, warum Sie in den letzten 12 Monaten keine Waren oder Dienstleistungen über das Internet bezogen haben?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- ☐ Fehlender physischer Kontakt mit dem Produkt
- ☐ Führen von Kundenprofilen: Speicherung von Interessen und Bestellhistorie
- ☐ Registrierungszwang: Angabe von persönlichen Daten
- ☐ Unsichere Verbindung: Wahrung der Privatsphäre
- ☐ Angst vor Datendiebstahl: Fehlender Datenschutz
- ☐ Angst vor finanziellem Schaden
- ☐ Kein Bedarf
- ☐ Sonstiges:

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

FERDINAND PORSCHE
FERN FH

18% ausgefüllt

2. Welche Vorteile des E-Commerce stellen für Sie persönlich eine Motivation dar, Online einzukaufen?

	wenig motiverend				stark motivierend	Kein Vorteil
Grenzüberschreitende Bezugsmöglichkeiten	○	○	○	○	○	○
Orts- und Zeitunabhängigkeit	○	○	○	○	○	○
Erleichterte Informationsbeschaffung und Preisvergleiche	○	○	○	○	○	○
Mobile Nutzungsmöglichkeit: Smartphone, Tablet o.ä.	○	○	○	○	○	○
Individualisierte Angebote	○	○	○	○	○	○
Express Liefermethoden: Same Day Delivery o.ä.	○	○	○	○	○	○

3. Welche Nachteile des E-Commerce haben Sie bereits erfolgreich von einem Kauf abgehalten?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- ☐ Fehlender physischer Kontakt mit dem Produkt
- ☐ Führen von Kundenprofilen: Speicherung von Interessen und Bestellhistorie
- ☐ Registrierungszwang: Angabe von persönlichen Daten
- ☐ Unsichere Verbindung: Wahrung der Privatsphäre
- ☐ Angst vor Datendiebstahl: Fehlender Datenschutz
- ☐ Angst vor finanziellem Schaden

4. Welche Bezahlmöglichkeiten bevorzugen Sie im Rahmen einer Online Transaktion?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- ☐ Vorkasse
- ☐ Lastschrift
- ☐ Kreditkarte
- ☐ Sofortüberweisung, Giropay
- ☐ PayPal
- ☐ ClickandBuy
- ☐ Guthabenkarten
- ☐ Sonstige:

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

27% ausgefüllt

5. Sofern Sie eine Kreditkarte für die Bezahlung nutzen, und der Anbieter keine TAN/Secure Code o.ä. Sicherheitsverfahren anbietet, führt dies Ihrerseits zu einem Kaufabbruch?

Anmerkung: Gemeint ist hier nicht der CVC Code bzw. Angaben direkt auf der Kreditkarte.

TAN/Secure Code Verfahren entsprechen u.a. von Ihnen selbst festgelegte Kennwörter, oder auch per SMS zugesandte Codes zur Freigabe einer Zahlung.

- ○ Ja
- ○ Nein
- ○ Nein, jedoch nur falls es an Alternativen mangelt

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

FERDINAND PORSCHE
FERN FH

36% ausgefüllt

6. Inwiefern treffen die folgenden Aussagen auf Sie persönlich zu?

Diese Frage dient der Erhebung Ihrer persönlichen Erfahrungen sowie einiger Grunddaten.

	niedrig				hoch
Online Kauferfahrung	○	○	○	○	○
Zufriedenheit im Umgang mit E-Commerce	○	○	○	○	○
Nutzungsdauer bzw. -intensität im E-Commerce	○	○	○	○	○
Selbstvertrauen im Umgang mit E-Commerce	○	○	○	○	○
Einkommen	○	○	○	○	○

7. Welche Faktoren stellen für Sie persönlich Gründe dar, von einem Online Kauf abzusehen?

	unerheblich				abschreckend
Fehlender physischer Kontakt	○	○	○	○	○
Mangelnde Reputation des Händlers	○	○	○	○	○
Versandrisiko	○	○	○	○	○
Aufwendungen durch Rückversand, Retoure o.ä.	○	○	○	○	○
Unsichere Bezahlmöglichkeiten	○	○	○	○	○
Verzögerungen im Bestellverlauf	○	○	○	○	○
Datenschutz	○	○	○	○	○
Unbekannte Marken: China Importe o.ä.	○	○	○	○	○

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

FERDINAND PORSCHE
FERN FH

38% ausgefüllt

7. Welche Authentifizierungsmethode(n) bevorzugen Sie, jeweils zusätzlich zu Benutzername bzw. E-Mail Adresse?

Bitte achten Sie auch auf die Anzahl der gemeinsam verwendeten Faktoren, Mehrfachnennungen sind möglich.

Bevorzugen Sie bspw. die gemeinsame Verwendung von Passwort + Biometrie, wählen Sie bitte beide Optionen aus.

- [ ] Passwort
- [ ] Biometrie (Fingerabdruck o.ä.)
- [ ] Token (Code per SMS, Smartphone App o.ä.)

8. Nutzen Sie eine E-Commerce Plattform dennoch, auch wenn diese nicht Ihrer bevorzugten Authentifizierungsmethode entspricht?

- ○ Ja
- ○ Ja, jedoch nur falls es an Alternativen mangelt
- ○ Nein

9. Verwenden Sie identische Passwörter für mehrere Plattformen?

- ○ Ja
- ○ Ja, jedoch nur für unbedenkliche Plattformen ohne E-Commerce Bezug
- ○ Nein

10. Welchen Stellenwert räumen Sie den Passwort-Mindestanforderungen der jeweiligen Plattform ein?

- ○ Ich halte mich stets an die Mindestvorgaben der jeweiligen Plattform.
- ○ Ich meide Plattformen mit zu komplexen Anforderungen an die Passwortstärke.
- ○ Ich übertreffe die Mindestvorgaben, um höhere Sicherheit zu erlangen.

11. Wie schätzen Sie die Passwortstärke Ihrer eigenen Passwörter ein?

- ○ Sehr sicher
- ○ Sicher
- ○ Durchschnittlich
- ○ Eher unsicher
- ○ Unsicher
- ○ Ich kann die Passwortstärke unmöglich einschätzen

12. Welche Eigenschaften der von Ihnen verwendeten Passwörter sind für Sie ein unverzichtbarer Bestandteil?
Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- ☐ Mindestanzahl an Zeichen
- ☐ Kleinbuchstaben
- ☐ Großbuchstaben
- ☐ Sonderzeichen
- ☐ Numerische Werte
- ☐ Numerische Werte und/oder Sonderzeichen in der Passwortmitte

13. Wie viele Zeichen entsprechen Ihren persönlichen Passwort-Mindestanforderungen?

☐ Zeichen

14. Ändern Sie die von Ihnen verwendeten Passwörter regelmäßig?

- ○ Ja
- ○ Ja, aber nur wenn es die Plattform zwingend vorgibt
- ○ Nein

15. Innerhalb welcher Zeit könnten nach Ihrer Einschätzung die folgenden Passwörter geknackt werden?
Das Ergebnis dieser Frage wird zu Ihrer Information auf der letzten Seite dieses Fragebogens angezeigt.

	Sofort	Minuten	Stunden	Tage/Wochen	Jahre/Jahrzehte
Hans123#	○	○	○	○	○
19_AnDaLa_90#	○	○	○	○	○
19_Anna_90#	○	○	○	○	○
Passwort1234	○	○	○	○	○
AAnnA1990$#	○	○	○	○	○

Weiter

FERDINAND PORSCHE
FERN FH

48% ausgefüllt

16. Achten Sie auf eine sichere Verbindung im Browser, sobald Sie eine E-Commerce Plattform nutzen?

- ○ Ich achte nicht auf Hinweise oder Schaltflächen im Zusammenhang mit IT-Sicherheit.
- ○ Ich achte auf eine HTTP Verbindung.
- ○ Ich achte auf eine HTTPS Verbindung.
- ○ Ich kann selbst nicht erkennen, ob eine sichere Verbindung vorliegt bzw. wie ich die Verbindungsart interpretieren soll.

17. Ist es Ihrer Einschätzung nach für einen Angreifer möglich, welcher Zugriff zu Ihrem System hat, Ihre komplette "Session", also Login/Passwort sowie Warenkorb zu übernehmen und in Ihrem Namen Bestellungen durchzuführen oder Ihre persönlichen Daten auszulesen?

- ○ Ja, dieses Risiko ist mir bewusst. Ich kann jedoch nicht sagen, wie ich mich davor schützen kann.
- ○ Ja, dieses Risiko ist mir bewusst. Ich lege jedoch keinen Wert auf Maßnahmen, welche mich davor schützen könnten.
- ○ Ja, dieses Risiko ist mir bewusst. Ich kenne entsprechende Maßnahmen, wie ich mich davor schützen kann.
- ○ Nein, davon habe ich noch nie etwas gehört.
- ○ Nein, davon habe ich noch nie etwas gehört. Ich kann mir aber vorstellen, dass dies ein relevantes Risiko darstellt.

18. Wie lautet Ihre Meinung zu der Verwendung von Cookies im Rahmen von E-Commerce Transaktionen?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- ☐ Ich akzeptiere grundsätzlich die Verwendung von Cookies und schätze die Vorteile die sich daraus ergeben.
- ☐ Ich akzeptiere grundsätzlich die Verwendung von Cookies, betrachte sie aber als Risiko.
- ☐ Ich achte auf die Art der verwendeten Cookies und überprüfe deren Sicherheitslevel manuell oder über Browser Plugins.
- ☐ Ich lehne die Verwendung von Cookies gänzlich ab, und deaktiviere Sie auch bei der Online Nutzung.
- ☐ Leider kann ich mit dem Begriff „Cookies" nichts anfangen.

19. Welche der folgenden Aussagen trifft auf Ihr An- und Abmeldeverhalten zu?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

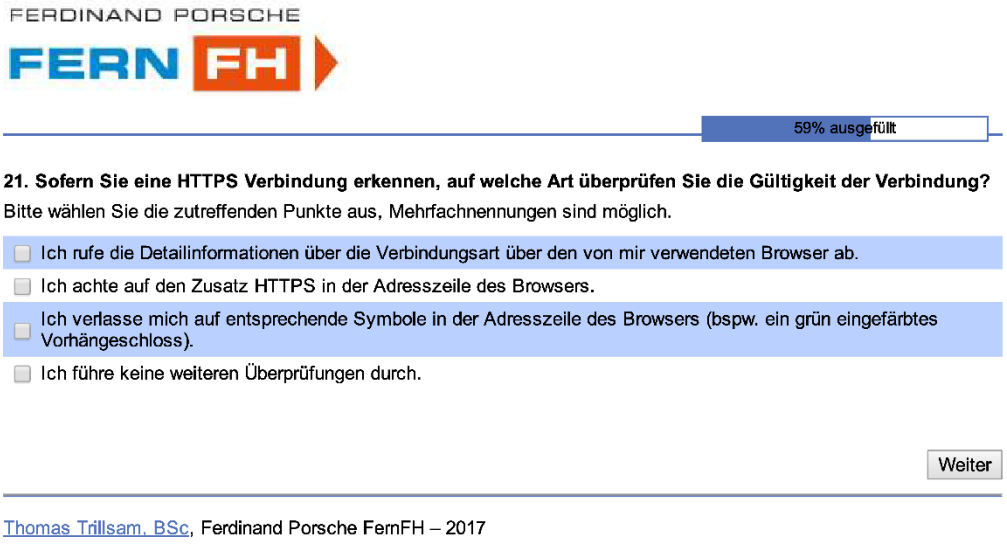
- ☐ Ich achte darauf, dass ich nach Verstreichen einer gewissen Zeitperiode automatisch abgemeldet werde (Session Timeout).
- ☐ Ich schätze es sehr, wenn mir die Zeitspanne bis zu einer automatischen Abmeldung visuell angezeigt wird (Stoppuhr o.ä.).
- ☐ Sollte ich nicht automatisch abgemeldet werden, führe ich den Abmeldevorgang manuell durch.
- ☐ Ich melde mich stets manuell ab, bevor ich die jeweilige Webseite verlasse.
- ☐ Sollte ich gefragt werden, ob ich "dauerhaft angemeldet bleiben möchte", wähle ich diese Option.
- ☐ Ich bevorzuge Webseiten, welche meine Anmeldung auch über den Neustart meines Endgerätes hinaus speichern.

20. Ist Ihnen die Funktionsweise von Zertifikaten bzw. deren Bedeutung für die Sicherheit einer E-Commerce Plattform bewusst?

- ○ Die Funktionsweise ist mir klar, mir ist es jedoch nicht möglich deren Sicherheitsstufe zu überprüfen.
- ○ Die Funktionsweise ist mir klar, und ich überprüfe auch regelmäßig die hinterlegten Zertifikate auf Sicherheit bzw. Gültigkeit.
- ○ Die Funktionsweise ist mir nicht klar, ich habe auch kein Interesse darauf zu achten.
- ○ Die Funktionsweise ist mir nicht klar, ich würde aber gerne mehr darüber erfahren.

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017


FERDINAND PORSCHE
FERN FH

59% ausgefüllt

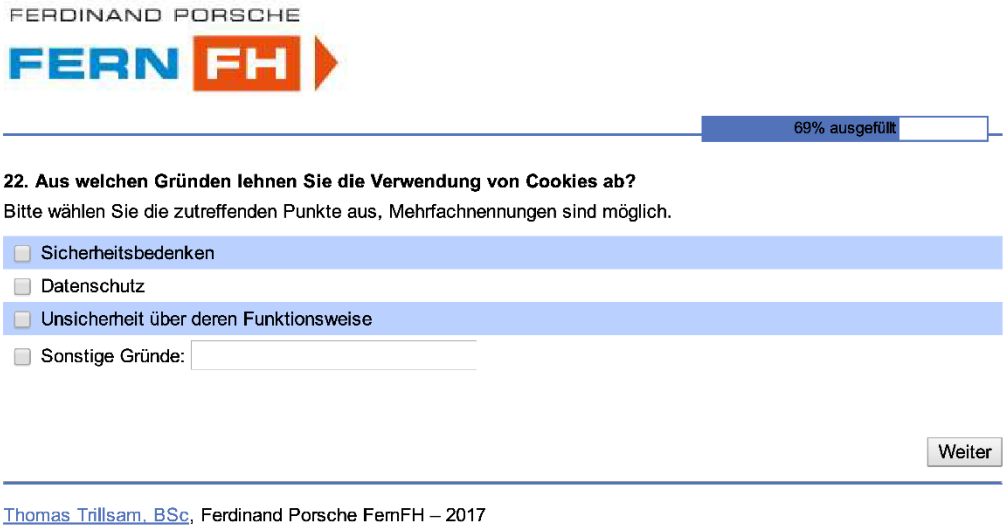
21. Sofern Sie eine HTTPS Verbindung erkennen, auf welche Art überprüfen Sie die Gültigkeit der Verbindung?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- [ ] Ich rufe die Detailinformationen über die Verbindungsart über den von mir verwendeten Browser ab.
- [ ] Ich achte auf den Zusatz HTTPS in der Adresszeile des Browsers.
- [ ] Ich verlasse mich auf entsprechende Symbole in der Adresszeile des Browsers (bspw. ein grün eingefärbtes Vorhängeschloss).
- [ ] Ich führe keine weiteren Überprüfungen durch.

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017


FERDINAND PORSCHE
FERN FH

69% ausgefüllt

22. Aus welchen Gründen lehnen Sie die Verwendung von Cookies ab?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- [ ] Sicherheitsbedenken
- [ ] Datenschutz
- [ ] Unsicherheit über deren Funktionsweise
- [ ] Sonstige Gründe:

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

FERDINAND PORSCHE
FERN FH

79% ausgefüllt

23. Welche Browser Erweiterungen bzw. Funktionalitäten nutzen Sie regelmäßig?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- [ ] Automatische Speicherung von Passwörtern
- [ ] Automatische Speicherung von Formulardaten
- [ ] Adobe Flash
- [ ] ActiveX
- [ ] Java
- [ ] Browser Plugins, welche Werbung, Skripte o.ä. blockieren
- [ ] Sonstige:
- [ ] Ich nutze keine Browser Erweiterungen bzw. Funktionalitäten

24. Welchen Stellenwert räumen Sie den folgenden Gütesiegeln bei der Verwendung von E-Commerce Plattformen ein?

	unbedeutend → zwingende Voraussetzung					Nicht bekannt
PCI-DSS	○	○	○	○	○	○
Trusted Shops	○	○	○	○	○	○
EHI Geprüfter Online-Shop	○	○	○	○	○	○
Verified by Visa/MasterCard	○	○	○	○	○	○
Österreichisches E-Commerce-Gütezeichen	○	○	○	○	○	○

25. Wie überprüfen Sie die Gültigkeit eines Gütesiegels?

Bitte wählen Sie die zutreffenden Punkte aus, Mehrfachnennungen sind möglich.

- [ ] Ich überprüfe lediglich, ob ein Gütesiegel sichtbar ist und führe keine weiteren Maßnahmen durch.
- [ ] Ich überprüfe, ob für das angegeben Gütesiegel eine zugehörige Webseite existiert.
- [ ] Ich überprüfe die Webseite des Gütesiegel Anbieters auf einen Eintrag der jeweiligen E-Commerce Plattform.
- [ ] Ich lege keinen Wert auf Gütesiegel und achte auch nicht darauf.

Weiter

Thomas Trillsam, BSc, Ferdinand Porsche FernFH – 2017

FERDINAND PORSCHE
FERN FH

90% ausgefüllt

26. Bitte geben Sie Ihr Geschlecht an.

- Weiblich
- Männlich

27. Welcher Altersgruppe gehören Sie an?

- 16 bis 25 Jahre
- 25 bis 34 Jahre
- 35 bis 44 Jahre
- 45 bis 54 Jahre
- 55 bis 64 Jahre
- 65 Jahre oder älter

28. Welches ist der höchste Bildungsabschluss, den Sie besitzen?

- Pflichtschule
- Lehre
- Matura
- Hochschule/Universität

29. Wie hoch ist Ihr monatliches Nettoeinkommen?

- Weniger als € 1.000,-
- Zwischen € 1.000,- und € 1.999,-
- Zwischen € 2.000,- und € 2.999,-
- Zwischen € 3.000,- und € 3.999,-
- Mehr als € 4.000,-
- Keine Angabe

30. Leben Sie in Österreich?

- Ja
- Nein

Weiter

FERDINAND PORSCHE
FERN FH

Vielen Dank für Ihre Teilnahme!

Ich möchte mich ganz herzlich für Ihre Mithilfe bedanken.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

Abschließend noch die Ergebnisse der Frage nach der Zeitspanne, welche für das Hacken verschiedener Passwörter benötigt wird:

Passwort1234	Sofort
Hans123#	3 Minuten
AAnnA1990$#	11 Stunden
19_Anna_90#	10 Jahre
19_AnDaLa_90#	663 Jahre

Quelle: Cygnius Password Strength Test, aufrufbar unter https://apps.cygnius.net/passtest