Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Onlineshopping-Plattformen

Änderungshistorie

Tabelle 1 Änderungshistorie

Version	***Datum***	***Name***	***Beschreibung***
V1.0	06.02.2023	Lars Bartsch, Bundesamt für Sicherheit in der Informationstechnik Maximilian Barz, secuvera GmbH Neli Dilkova-Gnoyke, G.I.M. mbH Jasmin Henn, Bundesamt für Sicherheit in der Informationstechnik Kurt Imminger, G.I.M. mbH Katarina Kühn, Bundesamt für Sicherheit in der Informationstechnik Dr. Simone Renner, G.I.M. mbH Kathrin Schäberle, secuvera GmbH Alexandra Wachenfeld-Schell, G.I.M. mbH	Erstversion

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: referat-wg32@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

1 Ergebnisüberblick

Onlineshopping erfreut sich einer zunehmenden Beliebtheit und wird immer häufiger in Anspruch genommen. Auch die COVID-19-Pandemie hat diese Entwicklung noch einmal verstärkt. Die vorliegende Studie ergab, dass über 90 Prozent aller Personen, die generell über einen Internetzugang verfügen, zumindest gelegentlich bei Onlineshops einkaufen. Die Mehrheit davon kauft ein- oder mehrmals pro Monat im Internet ein. Das am häufigsten genutzte Endgerät ist hierbei das Smartphone.

Mit zunehmender Einkaufsfrequenz und der Nutzung durch die meisten Bevölkerungsgruppen rückt auch die Frage der Datensicherheit beim Onlineshopping bzw. der Schutz persönlicher Daten immer mehr in den Fokus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) möchte mit der vorliegenden Studie eine empirische Grundlage schaffen, auf deren Basis Fragen des Digitalen Verbraucherschutzes beantwortet werden und die Erkenntnisse für die weitere Sensibilisierung der Verbraucherinnen und Verbraucher zum Thema Datensicherheit beim Onlineshopping genutzt werden können. Im Rahmen der Studie kamen verschiedene Methoden zur Anwendung: Schwachstellenanalysen von ausgewählten Shop-Softwareprodukten lieferten aus technischer Sicht Erkenntnisse, ob und welche Sicherheitslücken nach der Installation, der Konfiguration und dem Betrieb eines Onlineshops bestehen. Durch eine repräsentative Bevölkerungsbefragung konnte aufgezeigt werden, was Verbraucherinnen und Verbraucher unter Datensicherheit beim Onlineshopping verstehen, inwiefern ein persönliches Risiko wahrgenommen wird und welche Schutzmaßnahmen bekannt sind und zur Anwendung kommen. Im Vorfeld halfen qualitative Interviews mit Expertinnen und Experten, die hierfür zu berücksichtigenden Inhalte zu identifizieren.

Festzuhalten ist zunächst, dass es für den Begriff der Datensicherheit beim Onlineshopping kein eindeutiges Verständnis gibt. Verbraucherinnen und Verbraucher nennen hier sowohl das sichere Verschlüsseln der Zahlungsdaten und des Login-Passworts für den Kundenbereich als auch das Verhindern eines unrechtmäßigen Einsehens oder der Weitergabe von persönlichen Daten. Auch, dass Informationen über den getätigten Einkauf nicht für Werbezwecke verwendet werden, wird in diesem Zusammenhang genannt. Dies zeigt, dass der Begriff keineswegs einheitlich belegt ist und im Rahmen der Kommunikation mit den Verbraucherinnen und Verbrauchern der genauen Erläuterung bedarf.

Mit 68 Prozent hat die Mehrheit der Befragten generell Bedenken beim Onlineshopping. Gefahren im Internet allgemein und beim Onlineshopping sehen die Verbraucherinnen und Verbraucher vor allem in Bezug auf den Diebstahl von Bank- bzw. Kreditkartendaten, dem Weiterreichen persönlicher Daten und einen möglichen Identitätsdiebstahl.

Rund ein Viertel der Befragten hat bereits negative Erfahrungen im Hinblick auf die Datensicherheit beim Onlineshopping gemacht. Außerdem besteht große Unsicherheit darüber, welche Auswirklungen das Entwenden bzw. unrechtmäßige Einsehen von Daten für die Betroffenen hätte: Etwa die Hälfte der Befragten wüsste dies nicht genau. Gleichzeitig ist die große Mehrheit (81 Prozent) allerdings der Meinung, dass das unrechtmäßige Einsehen oder Entwenden der eigenen Daten sehr wahrscheinlich negative Auswirkungen auf sie selbst hätte.

Deutlich erkennbar ist der Wunsch nach Orientierung unter Verbraucherinnen und Verbrauchern. 81 Prozent wünschen sich ein Siegel von einer unabhängigen dritten Stelle, welches die Sicherheit von Onlineshops bewertet.

Die qualitativen Interviews, die mit Verbraucherinnen und Verbrauchern geführt wurden, ergaben Hinweise darauf, dass diese im Fall von Datenleak-Vorfällen nicht in der Lage sind, einschätzen zu können, welcher Schaden genau für sie entsteht. Auch Expertinnen und Experten betonten, dass Verbraucherinnen und Verbraucher kein unmittelbares Schadenerlebnis haben, das zu einer höheren Sensibilisierung für das Thema führen könnte.

Die Studie zeigt aber auch, dass Verbraucherinnen und Verbraucher sich selbst beim Thema Datensicherheit beim Onlineshopping als durchaus informiert einschätzen. Wichtigste Informationsquelle für das Thema Datensicherheit ist das Internet, gefolgt vom eigenen sozialen Umfeld. Etwa die Hälfte der Befragten gaben

an, generelles Interesse am Thema zu haben; ebenfalls rund die Hälfte hat sich in der Vergangenheit schon einmal dazu informiert. Expertinnen und Experten gaben jedoch in Interviews zu bedenken, dass aufgrund der hohen technischen Komplexität des Themas für Verbraucherinnen und Verbraucher kaum eine Chance besteht zu erkennen, ob ihre Daten beim Onlineshopping sicher sind. Insofern sprechen sich diese dafür aus, dass Maßnahmen, die die Datensicherheit für Verbraucherinnen und Verbraucher erhöhen, für diese möglichst einfach anwendbar sein müssen. Viel mehr als die Nutzung komplexer und verschiedener Passwörter für unterschiedliche Accounts sei nicht zu verlangen. Die durchgeführten technischen Tests verschiedener Software-Produkte für die Erstellung eines Onlineshops ergaben in diesem Zusammenhang aber, dass die Konfiguration einer sicheren Passwortrichtlinie häufig gar nicht möglich war. Die Mehrzahl der geprüften Shop-Softwareprodukte bot die Konfiguration der Passwortrichtlinie nicht oder nur unzureichend an. Die Softwarehersteller kommen damit ihrer Verantwortung für eine sichere Konfiguration des Onlineshops im laufenden Betrieb nicht nach. Es fällt außerdem auf, dass die Konfiguration einer Zwei-Faktor-Authentisierung als zusätzlicher Schutz des Verbraucherkontos in der Regel nicht möglich war.

Insgesamt kennt die Mehrheit der Befragten eine oder mehrere Maßnahmen zum Schutz der persönlichen Daten beim Onlineshopping, und ein Großteil davon wendet diese auch an. Beispielsweise die angesprochene Nutzung komplexer Passwörter oder den expliziten Logout nach der Onlineshop-Nutzung.

Mit Blick auf die Wahrnehmung der Verbraucherinnen und Verbraucher in Bezug auf die Information durch staatliche Institutionen und dem empfundenen Schutzgefühl hinsichtlich der Datensicherheit beim Onlineshopping kann festgestellt werden, dass sich nur knapp ein Fünftel durch staatliche Institutionen als gut informiert und geschützt betrachtet. Auf der anderen Seite gaben gut die Hälfte der Befragten an, das BSI zu kennen und mehr als ein Drittel dieser hat die Webseite des BSI bereits einmal besucht.

Zusammenfassend kann konstatiert werden, dass Verbraucherinnen und Verbraucher nur ein eingeschränktes Bewusstsein für das Risiko beim Onlineshopping haben. Aus der Sicht der Mehrheit der Befragten ist der Onlineshop dafür verantwortlich, sich um die Sicherheit persönlicher Daten zu kümmern. Die Studie macht deutlich, dass die Beurteilungsfähigkeit von Verbraucherinnen und Verbrauchern noch gestärkt werden kann. Zwar geht die Mehrheit der Befragten davon aus, dass sich ein Verlust persönlicher Daten negativ auswirken könnte. Dennoch wüsste nur eine Minderheit, wohin sie sich im Schadensfall zu wenden hätten. In der Konsequenz vertrauen mit 60 Prozent die Mehrheit der Befragten großen Onlineshops mehr als kleinen Shops.

Bei der technischen Betrachtung (Schwachstellenanalyse von Shop-Softwareprodukten) lässt sich festhalten: In jeder geprüften Software ließen sich Schwachstellen identifizieren. Es wurden zehn zufällig ausgewählte Shop-Softwareprodukte einem Test zugeführt, wobei die Ergebnisse sehr heterogen ausfielen. Teilweise wiesen die Produkte nur wenige Schwachstellen mit eher geringen Risikograden auf, teilweise aber auch eine Vielzahl von Schwachstellen mit teils gravierenden Auswirkungen auf das Sicherheitsniveau.

Am häufigsten traten Schwachstellen auf, die potenziell eine Übertragung sensibler Verbraucherdaten aus Formularfeldern an Dritte ermöglichten. Eine Passwortrichtlinie, die nicht oder nur unzureichend konfiguriert werden konnte, war die am zweithäufigsten identifizierte Schwachstelle. JavaScript-Bibliotheken von Drittanbietern, die verwundbar gegenüber bekannten Schwachstellen sind, waren ebenfalls häufig im Einsatz.

Im sich anschließenden Coordinated Vulnerability Disclosure-Prozess (CVD-Prozess) hat das BSI die Ergebnisse der Schwachstellenanalysen an die jeweiligen Hersteller übermittelt. Der CVD-Prozess war zum Zeitpunkt der Berichtlegung noch nicht abgeschlossen. In einigen Fällen haben die Hersteller zeitnahe Patches zur Verfügung gestellt wurden. Im Zuge dieses Prozesses übermittelten einige Hersteller Informationen darüber, dass bestimmte Schwachstellen durch eine sichere Konfiguration des Onlineshops vermeidbar gewesen wären. Es liegt daher der Schluss nahe, dass die Herstellerseite den Betreiberinnen und Betreibern von Onlineshops eine Handreichung zur Verfügung stellen muss, wie Onlineshops sicher zu installieren und einzurichten sind.

2 Hintergrund der Studie

2.1 Vorbemerkung

Der Digitalisierungsschub der letzten Jahre hat eine oft unzureichende Umsetzung von Anforderungen an die Sicherheit der Informationstechnik sichtbar gemacht. Dies manifestiert sich in zunehmenden Meldungen von Datenleak-Vorfällen, häufig bedingt durch Angriffe mittels Ransomware. Gerade Onlineshops sind aufgrund des immensen Umfangs an vorgehaltenen sensiblen Kundendaten im Fokus von Cyber-Kriminellen. Dies kann das Vertrauen von Verbraucherinnen und Verbrauchern in die Digitalisierung sowie in die Nutzung digitaler Produkte und Dienste nachhaltig mindern.

Gegenstand des vorliegenden Berichts ist eine mehrteilige Studie, die zum einen die Sicherheitseigenschaften ausgewählter Softwarelösungen im Onlineshopping (Shop-Software) untersucht und zum anderen das Bewusstsein von Verbraucherinnen und Verbrauchern für Datensicherheit beim Onlineshopping abfragt.

- Dafür wurde ein Überblick über einschlägige Shop-Softwareprodukte auf dem Verbrauchermarkt in Deutschland erarbeitet. Daran schloss sich eine technische Untersuchung (Penetrationstests) zur Analyse der Sicherheitseigenschaften ausgewählter Softwarelösungen an. Im Fokus stand der effektive Schutz von Kundendaten.
- Der Bericht enthält außerdem Bewertungen aus qualitativen Interviews sowohl mit Expertinnen und Experten als auch mit Verbraucherinnen und Verbrauchern und fasst Erkenntnisse aus einer umfassenden bevölkerungsrepräsentativen Befragung zusammen.

Somit integriert der Bericht eine technische und eine Verbraucherperspektive. Diese beiden Teile der Studie sind in zwei getrennten Kapiteln dargestellt.

2.2 Ausgangslage und Zielsetzung

Das BSI registriert regelmäßig Meldungen von Datenleak-Vorfällen, d. h. dem Diebstahl bzw. der Offenlegung von Daten, die nicht für die Öffentlichkeit bestimmt oder geeignet sind. Außerdem sind die Ursachen für Datenleak-Vorfälle gemäß den Beobachtungen des BSI oftmals nicht auf fortschrittliche Angriffsszenarien zurückzuführen, sondern auf die Ausnutzung von Sicherheitslücken der eingesetzten Shop-Software.

Diese Hintergründe und der durch die COVID-19-Pandemie ausgelöste Digitalisierungsschub waren Anlass für das BSI, eine Studie zur Datensicherheit im Onlineshopping in Auftrag zu geben. Ziel der Studie war der Gewinn evidenzbasierter Informationen, zu den auf dem deutschen Markt gängigen Onlineshopping-Plattformen und zu den spezifischen Bedürfnissen, Erwartungen, Wahrnehmungen und Verhaltensweisen von Verbraucherinnen und Verbrauchern bei konkreten Datenleak-Vorfällen. Das Risikobewusstsein, die wahrgenommene Beurteilungsfähigkeit und die vermutete Lösungskompetenz der Verbraucherinnen und Verbraucher standen ebenfalls im Mittelpunkt.

Um Erkenntnisse über den Wissenstand von Verbraucherinnen und Verbrauchern sowie ihrer Einschätzung von Risiken und ihrer Wahrnehmung von möglichen Schutzmaßnahmen zu erfassen, bezieht die Studie einen sozialpsychologischen Ansatz als Modell mit ein, nämlich das Extended Parallel Process Model (EPPM) von Witte (1992). Auf dieser Basis lassen sich differenzierte Kommunikationsmaßnahmen entwickeln, die den Wissenstand, den Umgang mit Risiken und die Selbsteinschätzung zur Gefahrenabwehr der Verbraucherinnen und Verbraucher berücksichtigen. Diese Komponenten werden vom EPPM systematisiert. Wie ein externer Stimulus wahrgenommen und darauf reagiert wird, hängt nach diesem Modell davon ab, wie die wahrgenommene Bedrohung (perceived threat) und die wahrgenommene Selbstwirksamkeit (self-efficacy) bzw. Wirksamkeit der Handlung (response efficacy) ausfallen. Je nach Ausprägung und Zusammenspiel werden entweder Prozesse in Gang gesetzt, die darauf abzielen, die Gefahr zu kontrollieren (danger control processes), wie z.B. die Verwendung eines Passwortmanagers, oder die

entstandene Angst zu kontrollieren (fear control processes), wie z.B. die Verhaltensweise, das Problem herunterzuspielen. Dieses Modell kann helfen, mögliche Reaktionen der Verbraucherinnen und Verbraucher vorwegzunehmen.

In der folgenden Abbildung 1 ist das EPPM schematisch dargestellt:

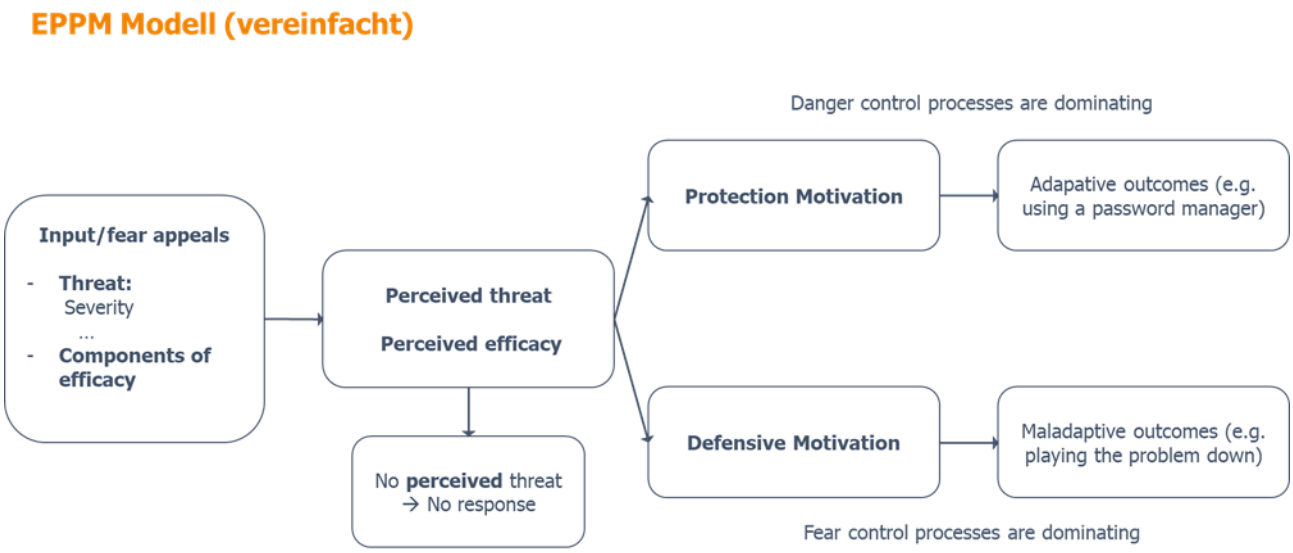


Abbildung 1 Vereinfachte Darstellung des Extended Parallel Process Model (EPPM) in Anlehnung an Witte (1992)

Es gilt also die Frage zu beantworten, wie Gefahrenkommunikation umgesetzt werden kann ohne Verbraucherinnen und Verbraucher zu überfordern oder abzuschrecken, sondern zu konstruktivem Handeln im Sinne des Selbstschutzes anzuleiten.

2.3 Aufbau und Methodik der Studie

Die vorliegende Studie kombiniert Ergebnisse auf Basis von sozialwissenschaftlichen Methoden und von IT-sicherheitstechnischen Analysen. Dies wurde über zwei Dienstleister abgedeckt. Die technischen Aspekte (Markt- und Schwachstellenanalyse) von der secuvera GmbH sind in Kapitel 3 enthalten. Die sozialwissenschaftlichen Aspekte (qualitative Befragung von Themen-Expertinnen und -Experten sowie die Verbraucherbefragung) von der G.I.M. – Gesellschaft für innovative Marktforschung mbH finden sich in Kapitel 4. Abbildung 2 veranschaulicht den Aufbau und den Methodenmix dieser Studie:

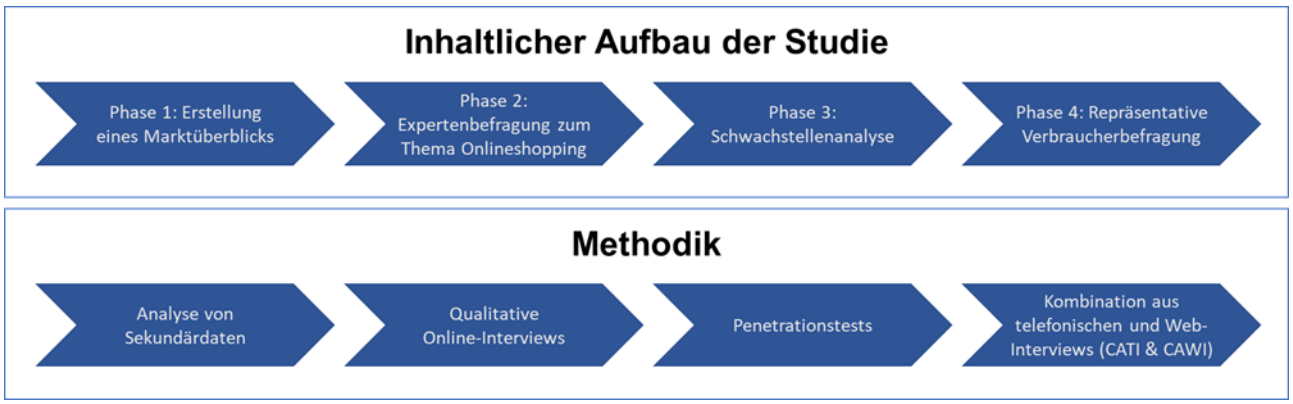


Abbildung 2 Schematischer Ablauf der Studie

Im ersten Schritt erfolgte eine Analyse zu den auf dem deutschen Markt gängigen Shop-Softwareprodukten. Für die Erstellung eines Marktüberblicks wurden diese anhand unterschiedlicher Merkmale kategorisiert. Übersichten über bereits bekannte Schwachstellen von Shop-Softwareprodukten und Datenleak-Vorfälle beim Onlineshopping ergänzten den Marktüberblick.

Die Aufgabe der Befragungen von Expertinnen und Experten zum Thema Onlineshopping war im nächsten Schritt unter anderem, den Marktüberblick zu validieren. In den dazu anberaumten qualitativen Interviews bekamen die befragten Expertinnen und Experten einen kurzen Einblick in die geleisteten Vorarbeiten, um sichergehen zu können, dass die Kategorisierung der Shop-Software ein möglichst repräsentatives Abbild des Marktes wiedergibt und somit eine valide Arbeits- und Entscheidungsgrundlage vorliegt. Außerdem fanden vier Interviews mit Verbraucherinnen und Verbrauchern statt, um deren Wahrnehmung, Einstellungen, Verhaltensweisen beim Onlineshopping zu erfassen. Auf dieser Basis wurde der Fragebogen für die Verbraucherbefragung im nächsten Arbeitsschritt mit relevanten Fragen und Statements ergänzt.

Die Auswahl der elf Themen-Expertinnen und -Experten sollte garantieren, dass unterschiedliche Aspekte über die Interviews abgedeckt sind. Einerseits sollten einige Teilnehmende einen technisch fundierten Einblick in das Thema Datensicherheit beim Onlineshopping haben. Andererseits sollten bei der Befragung auch Teilnehmende mit einer geeigneten fachlichen Einschätzung zur Situation der Verbraucher integriert sein.

Letztlich sollte die Expertenauswahl auch ein besseres Verständnis der Perspektive der Onlinehändler ermöglichen.

Tabelle 2 Überblick über die qualitativen Interviews mit den elf Expertinnen und Experten

Gruppe 1: Technisch versierte Expertinnen und Experten	***Gruppe 2: Expertinnen und Experten mit einem fundierten Blick auf die Verbraucherinnen und Verbraucher***	***Gruppe 3: Betreiberinnen und Betreiber eines eigenen Webshops***
Michael Gabler (7-it eG)	Stefanie Siegert (Teamleiterin Digitales, Energie & Mobilität, Landesgeschäftsstelle Verbraucherzentrale Sachsen)	Zwei Betreiber von Onlineshops
Ein Programmierer (Angestellter in einem mittelständischen Pharma-Unternehmen, hausintern für die Erstellung des Onlineshops zuständig)	Dr. Ayten Öksüz (Referentin Datenschutz und Datensicherheit Gruppe Verbraucherrecht, Verbraucherzentrale NRW e.V)	
Winfried Schneller (selbständiger Unternehmer und angestellt im Bereich Software-Entwicklung)	Prof. Dr. Timo Jakobi (Technische Hochschule Nürnberg)	
Andreas Sachs (Bereichsleiter Cybersicherheit und Technischer Datenschutz, Vizepräsident Bayerisches Landesamt für Datenschutzaufsicht)	Dr. Stephan Telschow (Gesellschaft für Innovative Marktforschung)	
Jan Mahn (Heise-Verlag)		

Auf Basis des Marktüberblicks wurden per Zufallsstichprobe zehn Shop-Softwareprodukte für Schwachstellenanalysen ausgewählt. Für jede dieser Untersuchung erstellte die secuvera GmbH einen Ergebnisbericht mit den identifizierten Schwachstellen und Sicherhinweisen in den getesteten Produkten. Diese Ergebnisberichte hat das BSI im Rahmen des CVD-Prozesses im Anschluss an die jeweiligen Hersteller übermittelt.

Im letzten Schritt der Studie fand eine repräsentative Befragung statt, um Verhalten und Einstellungen von Verbraucherinnen und Verbrauchern sowie ihre Perspektive auf das Thema Datensicherheit im Onlineshopping zu erfassen.

3 Markt- und Schwachstellenanalyse von Shop-Software

3.1 Marktanalyse

3.1.1 Marktsichtung und Produktkriterien

Im Zuge der Marktanalyse ermittelte das Projektteam zunächst, die am Markt vorhandenen Shop-Softwareprodukte und unterzog diese im Anschluss einer Marktsegmentierung. Im Fokus der Marktanalyse stand Shop-Software auf dem Verbrauchermarkt in Deutschland. Zudem sollte es sich bei den Plattformen um On-Premise Software handeln, welche auf Systemen installiert und ausgeführt wird, die eine jeweilige Betreiberin oder ein Betreiber selbst verantwortet. Shop-Software, die in Cloud-Umgebungen betrieben wird, war nicht Bestandteil der Analyse.

Ziel war es, das Angebot von Shop-Software in Teilbereiche einzuteilen und möglichst sicherheitstechnische Kriterien für die Segmentierung festzulegen. In den folgenden Abschnitten werden die Kriterien und deren sicherheitstechnische Relevanz erläutert.

Art der Lösung: In dieser Kategorie wurde unterschieden zwischen Open Source und proprietärer Software. Weiter unterteilte das Projektteam die Art der Lösung in Standalone- und Plugin-Software. Bei Open Source Software ist der Quelltext öffentlich zugänglich und kann eingesehen werden. Bei proprietärer Software ist der Quellcode in der Regel unter Verschluss und nicht frei zugänglich. Im Fall von Standalone-Lösung erfolgt der Betrieb als Komplettpaket. Plugin-Software kann als eine Zusatzsoftware, beispielsweise in ein Content-Management-System (CMS), eingebunden werden.

Die Art der Lösung wurde als besonders sicherheitsrelevant eingestuft, da der Quellcode von Open Source Software potenziell von jeder Person eingesehen und auf Schwachstellen untersucht werden kann. Dies kann dazu führen, dass bei Open Source Software mehr Schwachstellen bekannt werden, weil grundsätzlich jede interessierte Person eine Analyse des Source-Codes durchführen könnte.

Bei proprietärer Software ist der Quellcode nicht zugänglich, so dass Quellcode-Analysen hier durch den Hersteller selbst oder einen beauftragten Sicherheitsdienstleister erfolgen müssen. Sicherheitsexpertinnen und -experten identifizieren Schwachstellen in proprietärer Software daher in der Regel in einem Black-Box Ansatz.

Der Betrieb als Komplettpaket oder als Plugin in einem CMS entfaltet eine sicherheitstechnische Relevanz, wenn Schwachstellen, die im CMS bekannt werden, auch Auswirkungen auf die Sicherheit von Verbraucherdaten in der Plugin-Software haben.

Headless-Option: Alle gefundenen Lösungen liefern grundsätzlich eine graphische Benutzeroberfläche (GUI) mit. Einige Lösungen am Markt verfügen zusätzlich über eine Headless-Option. Dies bedeutet, dass die Lösung so betrieben werden kann, dass lediglich das Shop-Backend verwendet werden muss und die grafische Oberfläche selbst entwickelt oder eine Dritt-Software eingesetzt werden kann. Da eine klare Trennung zwischen Front- und Backend existieren muss, können spezialisierte Entwicklungsteams gebildet werden. Für die Sicherheit kann dies insofern bedeuten, dass die Entwicklung von Front- und Backend entkoppelt voneinander erfolgen kann und stärker auf die jeweilige Technologie spezialisiert ist. Im Umkehrschluss muss IT-Sicherheit sowohl im Front- als auch im Backend implementiert werden.

Die folgende Tabelle stellt die im Rahmen der Marktanalyse betrachteten Produkte und deren Eigenschaften tabellarisch dar.

Tabelle 3 Betrachtete Softwarelösungen

Name der Lösung	*Art der Lösung*	*Headless Option*
commerce:seo	Open-Source[1] (Standalone)	nicht bekannt
CosmoShop	Proprietäre Software[2] (Standalone)	nein
Etailer E-Commerce	Proprietäre Software (Standalone)	nein
Gambio	Proprietäre Software (Standalone)	nicht bekannt
H.H.G Multistore	Open-Source (Standalone)	nein
HCL Commerce	Open-Source (Standalone)	nicht bekannt
Ibexa	Proprietäre Software (Standalone)	ja
JTL	Open-Source (Standalone)	ja
Magento	Open-Source (Standalone)	nein
Merconis for Contao	Open-Source (Standalone)	ja
modified eCommerce Shopsoftware	Open-Source (Standalone)	nicht bekannt
MONDO MEDIA	Proprietäre Software (Standalone)	nein
nopCommerce	Open-Source (Standalone)	nein
Opencart	Open-Source (Standalone)	ja
OROCOMMERCE	Open-Source (Standalone)	nein
osCommercer	Open-Source (Standalone)	nein
OXID eSales	Open-Source (Standalone)	nein
PrestaShop	Open-Source (Standalone)	nein
Shopware	Open-Source (Standalone)	ja
Smartstore	Open-Source (Standalone)	ja
Spree Commerce	Open-Source (Standalone)	ja
Sylius	Open-Source (Standalone)	ja
VirtueMart	Open-Source (Plugin)	nein
WooCommerce	Open-Source (Plugin)	nein
wpShopGermany	Open-Source (Plugin)	nein
xanario	Proprietäre Software (Standalone)	nein
XONIC Shopsoftware	Proprietäre Software (Standalone)	nein
xt:commerce	Proprietäre Software (Standalone)	nein
Zen Cart	Open-Source (Standalone)	nein

3.1.2 Bekannte Schwachstellen und Datenleaks

Für die betrachteten Softwarelösungen recherchierte und analysierte das Projektteam die bekannt gewordenen Datenleak-Vorfälle und Schwachstellen der letzten fünf Jahre. Unter Datenleak-Vorfällen sind hierbei Ereignisse gemeint, bei denen Verbraucherdaten, wie beispielsweise Zugangsdaten oder personenbezogene Daten offengelegt wurden. Zur Informationsgewinnung und Recherche verwendete das Team öffentliche Schwachstellendatenbanken sowie die jeweiligen Hersteller-Webseiten.[3,4]

Für die genannten Shop-Softwareprodukte konnte eine Gesamtanzahl von über 400 Schwachstellen in den letzten fünf Jahren ermittelt werden. Schwachstellen werden in der Regel bei der Veröffentlichung mithilfe des CVSS (Common Vulnerability Scoring System) bezüglich ihrer Kritikalität eingestuft.[5] Der CVSS ist der

[1] Open Source in der Community Edition
[2] Auf GitHub sind Projektinformationen und Quelltext vorhanden. Der letzte Commit liegt jedoch mehrere Jahre zurück, daher wird die Software als oroprietär eingestuft.
[3] https://nvd.nist.gov/vuln
[4] https://cve.mitre.org/index.html
[5] https://www.first.org/cvss/

Industriestandard zur Bewertung von Schwachstellen und wurde von der Organisation FIRST (Forum of Incident Response and Security Teams) entwickelt. Die gefundenen Schwachstellen, inklusive deren Kritikalität, wurde in einer Übersicht erfasst. Auf Basis der öffentlich verfügbaren Informationen erfolgte eine Einstufung der Schwachstellen hinsichtlich der Auswirkungen auf die Sicherheit von Verbraucherdaten.

Von den insgesamt 418 öffentlich bekannten Schwachstellen innerhalb der letzten fünf Jahre wiesen hierbei 28 Schwachstellen einen kritischen Risikograd auf. Einen hohen Risikograd wiesen 87 identifizierte Schwachstellen auf. Die deutliche Mehrheit der Schwachstellen wurde mit einem mittleren Risikograd eingestuft. 66 Schwachstellen besaßen einen niedrigen Risikograd. Es handelte sich in den meisten Fällen um Sicherheitslücken, die im Zusammenhang mit verwendeten Software-Bibliotheken stehen, für die Schwachstellen öffentlich bekannt sind. Weiterhin wurden eine Vielzahl an Schwachstellen veröffentlicht, die im Zusammenhang mit der Umgehung von Zugangskontrollen stehen, sowie Sicherheitslücken, die geeignet sind, eigenen Code in den Onlineshop einzubringen (*Injection*-Schwachstellen).

Teilweise liegen für veröffentlichte Schwachstellen keine tiefgehenden Informationen vor, so dass in diesen Fällen keine zuverlässige Einstufung erfolgen konnte. Die Mehrheit der Schwachstellen stufte das Projektteam als direkte oder potenzielle Gefährdung der Sicherheit von Verbraucherdaten ein. Bei nur 80 der 418 bewerteten Schwachstellen traf das Projektteam das Votum, dass diese Schwachstellen keine direkte Auswirkung auf die Sicherheit von Verbraucherdaten hatten.

Anschließend fand eine Analyse von konkreten Datenleak-Vorfällen der letzten fünf Jahre statt, welche Auswirkungen auf Verbraucherinnen und Verbraucher aus Deutschland hatten. Hierzu führte das Projektteam ebenfalls eine Online-Recherche durch und analysierte, welche Datenleak-Vorfälle in der Vergangenheit im Kontext von Onlineshopping bereits aufgetreten sind. Die Quellen, die für die Recherche herangezogen wurden, waren hierbei vielfältig. Zum einen wurden Meldungen der Hersteller berücksichtigt, zum anderen aber auch Pressemeldungen.

Im Zuge der Analyse stellte das Projektteam fest, dass es in den letzten fünf Jahren eine Vielzahl von Datenleak-Vorfällen auf dem deutschen Verbrauchermarkt gab. Allein im Jahr 2022 waren zum Zeitpunkt der Recherche acht Vorfälle im Kontext von Onlineshopping bekannt, die Auswirkungen auf die Datensicherheit von Verbraucherinnen und Verbrauchern aus Deutschland hatten. Die Gründe für die einzelnen Vorfälle waren vielfältig, jedoch lassen sich diese in vielen Fällen auf technische Schwachstellen zurückführen.

Ein Beispiel hierfür ist ein Datenleak-Vorfall aus dem Januar 2022, bei dem durch einen Brute-Force-Angriff auf die Anmeldemaske des betroffenen Online-Shops Zugang zu Kundenkonten erlangt werden konnte.[6] Bei dieser Angriffsmethode versucht eine Angreiferin bzw. ein Angreifer Zugangsdaten (hier Benutzername und Passwort) durch vielfaches Ausprobieren zu erraten. Bei diesem konkreten Fall konnten die Angreiferinnen bzw. Angreifer Zugang zu Kundenkonten im mittleren fünfstelligen Bereich erlangen.

Zwei weitere Datenleak-Vorfälle zu Beginn des Jahres 2022 waren auf Injection-Verwundbarkeiten der betroffenen Shop-Software zurückzuführen. Hierbei waren die Angreiferinnen und Angreifer in der Lage, schadhafte Inhalte an die Anwendung zu übergeben und eigenen Code darin auszuführen. In einem Fall konnten sie durch eine SQL-Injection personenbezogene Daten in großem Umfang auslesen.[7] Laut Recherche sollen 300.000 Online-Shops von der Lücke betroffen gewesen sein. In einem anderen Fall konnten die Angreiferinnen und Angreifer über eine Cross-Site-Scripting-Verwundbarkeit (XSS) auf Adressdaten zugreifen.[8] Auch hier waren sie durch die Ausnutzung der XSS-Schwachstelle in der Lage, eigenen Code in der Anwendung auszuführen.

[6] https://www.heise.de/news/Brute-Force-Angriff-Mittlere-fuenfstellige-Zahl-von-thalia-de-Konten-gehackt-6336552.html

[7] https://thehackernews.com/2022/07/hackers-exploit-prestashop-zero-day-to.html

[8] https://www.heise.de/news/Datenleck-im-Shopsystem-von-Tuxedo-Computers-6496131.html

Ein weiterer Vorfall aus dem Jahr 2022 bezieht sich auf einen Online-Shop, in dem mutmaßlich mehrerer 100.000 Buchungsbestätigungen, inklusiver sensibler Daten, wie beispielsweise E-Mail-Adressen und Adressdaten, ungeschützt und direkt aufrufbar im Internet verfügbar waren.[9]

Der Großteil der Ursachen für die Datenleak-Vorfälle lässt sich auf technische Schwachstellen in den verwendeten Plattformen zurückführen. Ein Mittel um die Gefahr von zukünftigen Datenleak-Vorfällen zu vermindern, stellen daher Schwachstellenanalysen dar, die regelmäßig sowie im besten Fall bereits im Entwicklungszyklus durchgeführt werden.

3.2 Planung der Schwachstellenanalysen

3.2.1 Produktauswahl

Die folgenden zehn Shop-Softwareprodukte wurden durch eine Zufallsauswahl für die Schwachstellenanalyse ermittelt:

- commerce:seo,
- Gambio,
- Magento,
- Merconis für Contao,
- Prestashop,
- Shopware,
- Sylius,
- wpShopGermany,
- XONIC Shopsoftware,
- Zen Cart.

3.2.2 Vorgehensweise zur Prüfung

3.2.2.1 Installation

Durch die Zufallsauswahl wurde vor allem Shop-Software selektiert, die frei verfügbar ist und für die dementsprechend keine Lizenz notwendig war. In einigen Fällen konnte auf eine Testlizenz zurückgegriffen werden, welche die Hersteller zur Verfügung stellten. In einem Fall war ein Lizenzkauf erforderlich. Hervorzuheben ist, dass nahezu alle Hersteller sehr positiv auf die Ansprache des Projektteams reagierten, im Zuge der Installation der Testsysteme ansprechbar waren und auch Hilfe bei der Inbetriebnahme und Konfiguration anboten.

Zu Beginn jeder Installation wurde die jeweilig zu prüfende Shop-Software in eine für diesen Test vom Prüfer erstellte und konfigurierte lokale virtuelle Ubuntu-Maschine übertragen. Das Projektteam setzte für jede Prüfung zunächst einen Webserver mittels eines sogenannten LAMP-Stacks auf. Auf diesem wurde im Anschluss die Shop-Software, anhand der durch den jeweiligen Hersteller angebotenen Anleitung installiert. Stellte der Hersteller eine Anleitung zur Konfiguration oder eine Handreichung für eine sichere Konfiguration zur Verfügung, wurde die Konfiguration auf Basis dieser Dokumente vorgenommen.

3.2.2.2 Prüfungsvorgehen

Um eine Methodik für die Durchführung von Schwachstellenanalysen zu entwickeln, erstellte das Projektteam einen Angriffs- und Durchführungskatalog. Ziel dieser Kataloge war es, eine gleichbleibende

[9] https://www.heise.de/select/ct/2022/10/2209615223486987308

Güte der Tests und eine hohe Qualität sowie Vergleichbarkeit der einzelnen Prüfungen zu gewährleisten. Der Angriffskatalog beinhaltete eine Auflistung aller im Rahmen der Prüfung möglichen Angriffe auf die ausgewählten Testgegenstände. Die konkreten Prüfungen, welche auf die Shop-Software angewandt wurden, waren im Durchführungskatalog enthalten. Durch die Bearbeitung der einzelnen Angriffs- und Durchführungskataloge konnte stets ein Negativ-Reporting erstellt werden. Bei einem solchen Reporting werden alle Ergebnisse der durchgeführten Tests angegeben, auch wenn sie aus Sicht der Anwendung zu keiner Schwachstelle oder zu einem Fehler führen.

Als Basis für den Angriffs- und Durchführungskatalog wurde der *Web Security Testing Guide* der OWASP in Version 4.2 verwendet.[10] Es handelt sich hierbei um einen weit verbreiteten Standard, der sehr ausführlich die Vorgehensweise für die Identifizierung von Schwachstellen in Webapplikationen beschreibt. Im Rahmen der Definition des Angriffs- und Durchführungskatalogs glich das Projektteam ab, ob alle identifizierten Bedrohungen auf Prüfungen des OWASP *Testing Guides* abgebildet werden konnten. Dies sollte sicherstellen, dass alle identifizierten Gefährdungen in den durchzuführenden Schwachstellenanalysen Beachtung finden. Es existiert ein weiteres Dokument der OWASP, der *Application Security Verification Standard* (ASVS).[11] Dieses Dokument beinhaltet einen Testkatalog, der nicht nur an Sicherheitsexpertinnen und -experten gerichtet ist, sondern auch Hilfestellungen im Konzept einer sicheren Architektur und Entwicklung geben soll. Der *Testing Guide* berücksichtigt einige Punkte, wie beispielsweise die Multi-Faktor-Authentifizierung, nicht ausführlich. Aus diesem Grund wurden die beiden Standards miteinander abgeglichen, um noch fehlende Punkte und alle für das Projekt relevanten Prüfungen in den Angriffs- und Durchführungskatalog aufzunehmen. Der ASVS wurde in Version 4.0.3 verwendet.

Einige Prüfpunkte, die im *Testing Guide* und im ASVS vorgesehen sind, schloss das Projektteam für die Prüfungen der Softwareprodukte aus, da On-Premise-Produkte im Fokus standen. Es erfolgten keine Prüfungen der Infrastruktur und der Transportverschlüsselung.

Der Fokus der Prüfungen lag zum einen auf technischen Schwachstellen. Hierunter fallen beispielsweise Schwachstellen, die auf eine fehlerhafte Prüfung der Benutzereingaben zurückzuführen sind. Zum anderen erfolgte eine Prüfung des Berechtigungsmodells. In diesem Schritt prüfte das Projektteam, ob eine horizontale oder vertikale Rechteausweitung möglich war. Eine horizontale Rechteausweitung liegt beispielsweise dann vor, wenn ein Zugriff auf fremde Kundendaten erfolgen könnte. Eine vertikale Rechteausweitung liegt dann vor, wenn aus dem Kundenkontext auf Daten im Kontext des Administratoren-Bereichs zugegriffen werden könnte.

Die Prüfungen erfolgten zunächst vor allem automatisiert, mithilfe von *Burp Suite Pro*.[12] Je nach Szenario bezog das Projektteam weitere Werkzeuge in die Tests ein, um die automatisiert prüfbaren Tests des Durchführungskatalogs abzuarbeiten. Die Ergebnisse wurden im Nachgang manuell verifiziert und bewertet. Nach Abschluss der automatisierten Tests fanden manuelle Prüfungen gemäß des Durchführungskatalogs statt. Der jeweilige Tester erstellte pro durchgeführter Prüfung einen ausführlichen Ergebnisbericht, in dem alle gefundenen Schwachstellen, deren Auswirkungen und Behebungsempfehlungen beschrieben sind. Weiterhin wurde die entsprechende Testvorgehensweise festgehalten und bei Schwachstellen eine möglichst nachvollziehbare Schritt für Schritt Anleitung erstellt, um die gefundenen Schwächen nachvollziehen zu können.

Für die Penetrationstests wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“ zugrunde gelegt[13]:

[10] https://owasp.org/www-project-web-security-testing-guide/
[11] https://owasp.org/www-project-application-security-verification-standard/
[12] https://portswigger.net/burp/pro
[13] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.html

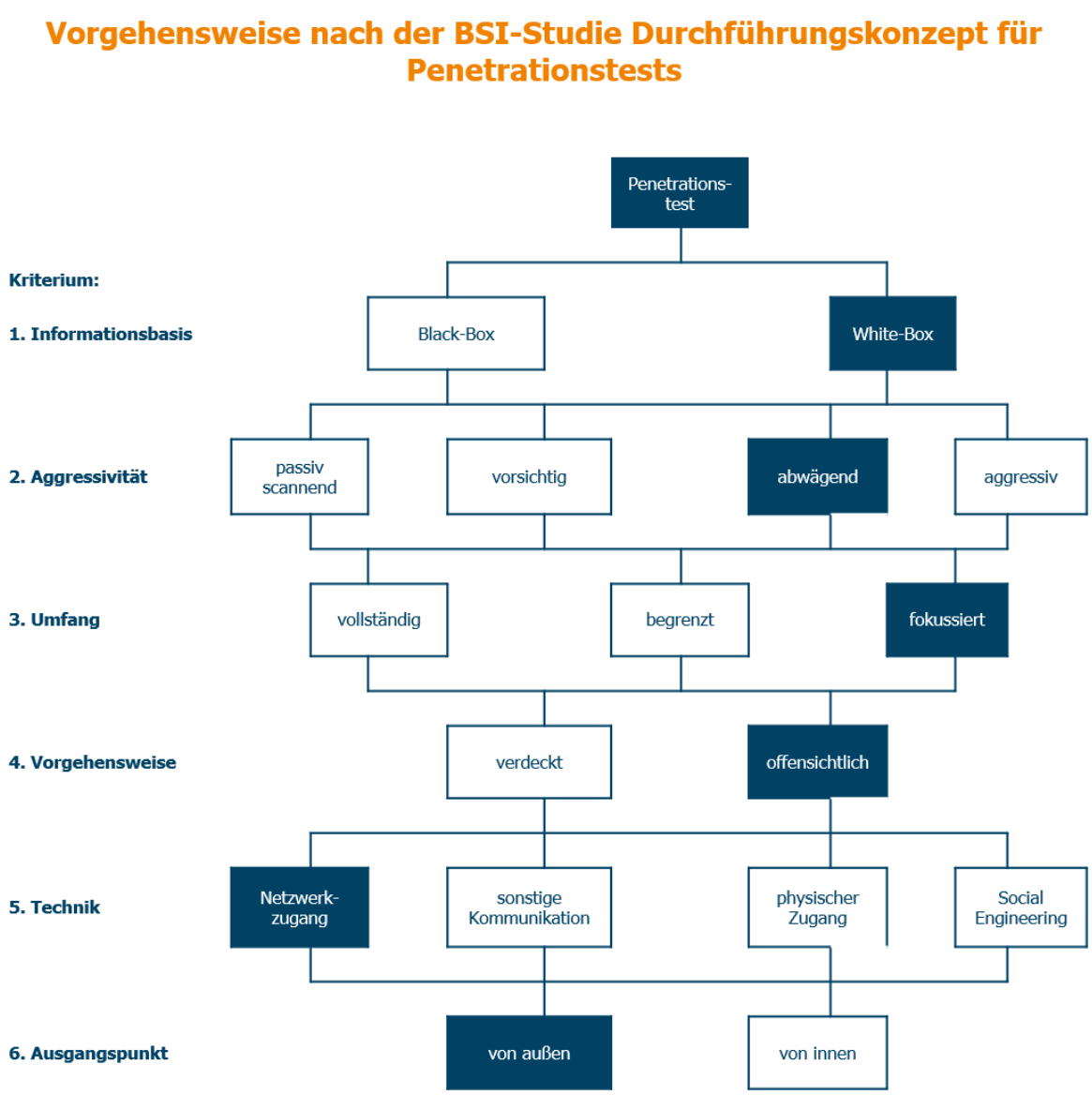


Abbildung 3 Vorgehensweise nach „Durchführungskonzept für Penetrationstests“

Das Kriterium Informationsbasis beschreibt die Wissensbasis des Projektteams für die Durchführung der Prüfung. Hier kann zwischen einem Black-- und White-Box-Ansatz unterschieden werden. Da die Shop-Software jeweils auf Systemen des Projektteams installiert wurde, lagen den Testern tiefgehende Informationen über diese und teilweise auch der Quellcode vor. Die Informationsbasis entsprach daher tendenziell eher der einer White-Box-Prüfung.

Für das Kriterium der Aggressivität wählte das Projektteam die Stufe abwägend. Für den Nachweis erfolgte eine Ausnutzung von einzelnen Schwachstellen. Es fanden jedoch keine destruktiven Angriffe, wie beispielsweise Denial-Of-Service-Angriffe statt.

Der Umfang der einzelnen Schwachstellenanalysen erfolgte fokussiert. Die ausgewählten Shop-Softwareprodukte stellen komplexe Anwendungen dar, die eine Vielzahl an Funktionen anbieten. Für die Tests begutachtete das Projektteam die Komponenten der Produkte, die sicherheitstechnisch von Interesse waren und eine Relevanz für die Sicherheit von Verbraucherdaten aufwiesen. Die Vorgehensweise war offensichtlich. Da das Projektteam die Lösungen selbst hostete, wurde nicht versucht, die Aktivitäten zu verschleiern.

Die Prüfungen erfolgten über einen Netzwerkzugang (Kriterium: Technik) und von außen (Kriterium: Ausgangspunkt), analog zu einem Angriff über das Internet.

3.2.2.3 Schwachstellenbewertung

Das Projektteam teilte die Schwachstellen in zwei Kategorien ein. Die erste Kategorie beinhaltete Schwachstellen, die aus Sicht der Prüfer ausnutzbar waren und einen direkten Einfluss auf die Sicherheit der Anwendung hatten. In der Regel brachte die Ausnutzung einer solchen Schwachstelle einen Vertraulichkeits- oder Integritätsverlust mit sich oder führte zu einer Einschränkung der Verfügbarkeit der Anwendung bzw. des kompletten Systems.

Bei der zweiten Kategorie handelte es sich um sogenannte Sicherheitshinweise. Während der Prüfung identifizierte das Projektteam Sicherheitsprobleme, die nicht klar als Schwachstelle zu bewerten sind, weil von ihnen kein direktes Risiko ausging oder es sich um Abweichungen von gängigen Sicherheitsstandards bzw. *Best-Practices* handelte, welche jedoch keinen direkten ausnutzbaren Angriff zur Folge hatten. Diese wurden lediglich als Hinweis eingestuft und bei der Ermittlung des Sicherheitsniveaus nicht weiter beachtet.

Zur Ermittlung des Risikograds von Schwachstellen kam das *Common Vulnerability Scoring*-System (CVSS) in Version 3.1 zum Einsatz.[14]

Für jede gefundene Schwachstelle berechnete das Projektteam den CVSS *Base Score* und nahm diesen Wert als Kritikalitätsbewertung der Schwachstelle in den Bericht auf. Der *Base Score* setzt sich zusammen aus den Voraussetzungen, die für einen erfolgreichen Angriff gegeben sein müssen (*Exploitability Metrics*) und den Konsequenzen, die die Ausnutzung der Schwachstelle mit sich bringen (*Impact Metrics*). Für die Voraussetzungen sind die folgenden Werte relevant:

- *Attack Vector*: In dieser Variable wird reflektiert, wie die Ausnutzung der Schwachstelle erfolgt. Beispielsweise wird hier unterschieden, ob eine Ausnutzung über ein Netzwerk oder lokal an der entsprechenden Komponente erfolgen muss.
- *Attack Complexity*: In den Werten *low* oder *high* wird die Komplexität des Angriffs bewertet. Ein Angriff, der wiederholbaren Erfolg verspricht, ohne dass besonderes Equipment oder Knowhow vorliegen muss, wird als niedrig komplex eingestuft. Während ein Angriff, der von Randbedingungen abhängt oder darauf begründet ist, dass sich eine Angreiferin bzw. ein Angreifer zunächst in die Umgebung einarbeiten muss, als *high* eingestuft wird.
- *Privileges Required*: In diese Variable wird reflektiert, ob der Angriff anonym erfolgen kann oder bestimmte Berechtigungen am entsprechenden Dienst vorliegen müssen.
- *User Interaction:* In einigen Fällen setzt die Ausnutzung von Schwachstellen an eine bestimmte Nutzerinteraktion mit dem verwundbaren Dienst voraus, beispielsweise ein Klick auf einen Link. Sollte dies der Fall sein, wird in dieser Kategorie der Wert *required* gesetzt.

Die Auswirkungen der Schwachstelle, wird anhand der folgenden Variablen bewertet:

- *Confidentiality Impact*: Ist dieser Wert gesetzt, bedeutet dies, dass die Ausnutzung der Schwachstelle zu einem Vertraulichkeitsverlust führt. Je nach Schwere, kann hier eine Einstufung in die Werte *high* oder *low* erfolgen.
- *Integrity Impact*: Ist dieser Wert gesetzt, bedeutet dies, dass die Ausnutzung der Schwachstelle zu einem Integritätsverlust führt. Je nach Schwere kann hier eine Einstufung in die Werte *high* oder *low* erfolgen.
- Availability Impact: Dieser Wert beschreibt eine Auswirkung der Ausnutzung der Schwachstelle auf die Verfügbarkeit. Analog zu den beiden obigen Variablen kann eine Einstufung in die Kategorien *high* oder *low* erfolgen, sofern die Verfügbarkeit des Dienstes oder des gesamten Systems beeinträchtigt ist.

Zusätzlich existiert die Variable *Scope*, welche die Auswirkungen eines Angriffs beschreibt. Hierbei kann der Wert *unchanged* gewählt werden, wenn die Schwachstelle lediglich Auswirkungen besitzt, die sich auf die

[14] https://www.first.org/cvss/calculator/3.1

Komponente selbst beziehen. Der Wert *changed* wird gewählt, falls noch weitere Komponenten existieren, auf die eine Ausnutzung der Schwachstelle Auswirkungen hat.

Das Projektteam bewertete jede Schwachstelle anhand der skizzierten Metriken, so dass sich auf Basis einer vorgegebenen Formel, der Base Score auf einer Skala von null bis zehn ergab. In der folgenden Tabelle ist die Zuweisung des ermittelten Wertes zu einem Risikograd abgebildet.

Tabelle 4 CVSS Base Score und zugeordneter Risikograd

Risikograd	***Base Score***
Geringer Risikograd	0.1 – 3.9
Mittlerer Risikograd	4.0 – 6.9
Hoher Risikograd	7.0 – 8.9
Kritischer Risikograd	9.0 – 10.0

3.3 Ergebnisse der Schwachstellenanalysen

Im Zuge der Schwachstellenanalysen konnte das Projektteam in jeder geprüften Shop-Software Schwachstellen identifizieren. Die Bandbreite reichte hierbei von sehr wenigen Schwachstellen bis hin zu sehr vielen Schwachstellen. In einem Fall konnten lediglich zwei Schwachstellen identifiziert werden, während in zwei anderen Fällen jeweils 17 Schwachstellen gefunden wurden.

Eine Schwachstelle trat in allen geprüften Produkten auf, während manche Schwachstellen hingegen auf individuelle Entwicklungsfehler zurückzuführen waren und daher nur in einer Shop-Software auftraten. Insgesamt konnten 30 verschiedene Schwachstellen im Rahmen der Prüfungen identifiziert werden. Da diese teilweise in mehreren Produktenvertreten sind, beträgt die Anzahl der insgesamt identifizierten Schwachstellen 78.

Der folgende Abschnitt fasst die Ergebnisse zusammen und stellt dies in einer Statistik übersichtlich dar.

3.3.1 Statistische Auswertung

Bei den am häufigsten aufgetretenen Schwachstellen handelt es sich um die Folgenden:

- **Mögliche Übertragung von sensiblen Informationen aus Formularfeldern an Dritte:** Diese Schwachstelle konnte in allen zehn Shop-Softwareprodukten identifiziert werden, besitzt jedoch lediglich einen geringen Risikograd. Sie bezieht sich darauf, dass es moderne Browser ermöglichen, Eingaben in Formularfeldern einer automatischen Rechtschreibprüfung während der Eingabe von Daten zu unterziehen. Dies geschieht entweder durch den Abgleich mit einem lokal im Browser installierten Wörterbuch (einfache Rechtschreibprüfung) oder unter Zuhilfenahme von meist Cloud-basierten Diensten (erweiterte Rechtschreibprüfung). Wird ein Cloud-basierter Dienst zur Prüfung verwendet, werden diese potenziell sensiblen Eingabedaten an den Browserhersteller oder Dritte gesendet. Die Vertraulichkeit der in die Anwendung eingegebenen Daten ist daher beeinträchtigt. Ein weiteres Attribut, das für alle Formularfelder mit möglicherweise sensiblen Nutzereingaben gesetzt werden sollte, ist autocomplete=off. Dieses verhindert, dass der Browser einmal getätigte Formulareingaben speichert und diese bei einem erneuten Aufruf der Seite durch eine fremde Person vorausfüllt.
- **Unzureichende Passwortrichtlinie:** In neun Fällen identifizierte das Projektteam eine unzureichende Passwortrichtlinie. Diese Schwachstelle wurde mit einem mittlerem Risikograd bewertet. Kann im Onlineshop keine oder nur eine unzureichende Passwortrichtlinie konfiguriert werden, sind die Kundenkonten schlecht geschützt. In den konkreten Testfällen wurde festgestellt, dass die Passwortrichtlinie in vielen Fällen nicht, oder nur unzureichend, konfigurierbar war und damit eine sichere Inbetriebnahme eines Onlineshops nicht möglich ist.

Verwundbare JavaScript-Bibliothek: In sieben Shop-Softwareprodukten beobachtete das Projektteam verwundbare JavaScript-Bibliotheken. Diese Schwachstelle, welche mit mittlerem Risikograd bewertet wurde, lässt sich darauf zurückführen, dass JavaScript-Bibliotheken von Drittanbietern eingesetzt werden, die verwundbar gegenüber bekannten Schwachstellen sind. Dies kann unter anderem dazu führen, dass eine Angreiferin bzw. ein Angreifer schadhaften Code in der Anwendung ausführen kann.

Administrator kann Kundenlogin umgehen: In fünf Fällen identifizierte das Projektteam Probleme, die sich auf die Funktionalität beziehen, über die eine Administratorin oder ein Administrator Aktionen im Onlineshop im Kundenkontext vornimmt. Da im Fokus dieses Projektes die Sicherheit von Kundendaten Gegenstand der Untersuchung war, lag hierbei vor allem die Protokollierung im Mittelpunkt der Prüfungen. Löst eine Administratorin oder ein Administrator im Auftrag einer Kundin oder eines Kunden beispielsweise eine Bestellung aus oder ändert Kundendaten, so sollte dies nachvollziehbar protokolliert werden. Im Zuge der Prüfungen konnte an einigen Stellen keine Protokollierung verifiziert werden, so dass dies als Schwachstelle aufgenommen wurde.

End-of-Life-Software im Einsatz: In ebenfalls fünf Shop-Softwareprodukten konnte Software identifiziert werden, die das offizielle End-of-Life-Datum (EOL) überschritten hat und dementsprechend nicht mehr durch den Hersteller unterstützt wird. EOL bedeutet, dass die Software keine Sicherheits-Updates, Bugfixes oder Sicherheitspatches mehr erhält und Verwundbarkeiten gegenüber diversen Schwachstellen vorliegen könnten. In der Regel handelte es sich hierbei um zusätzliche Software-Bibliotheken, die von den einzelnen Produkten eingebunden wurden. Auch erfolgt bei neu auftretenden Schwachstellen keinerlei Prüfung, ob diese in den abgelaufenen Software-Versionen zutreffend ist. Das Sicherheitsrisiko ist bei nicht mehr unterstützter Software daher unkalkulierbar und wurde mit sehr hohem oder kritischem Risikograd bewertet.

- **Dateien mit sensiblem Inhalt öffentlich erreichbar:** In vier Fällen waren Informationen öffentlich zugreifbar, deren Inhalt als sensibel eingestuft werden musste. Da die Informationen, auf die zugegriffen werden konnte je Onlineshop individuell waren, kann hier keine generelle Beschreibung des Risikograd erfolgen, da dies individuell für jede getestete Shop-Software erfolgte.

Die Schwachstellen mit dem höchsten Risikograd waren die Folgenden:

- **End-of-Life-Software im Einsatz:** Die Beschreibung dieser Schwachstelle erfolgte im obenstehenden Absatz.
- **Cross-Site-Request-Forgery-Angriffe (CSRF):** In einem Shop-Softwareprodukt bestand eine CSRF-Verwundbarkeit. Sofern es einer angemeldeten Angreiferin bzw. einem angemeldeten Angreifer gelingt, dass eine Administratorin oder ein Administrator auf einen manipulierten Link klickt, können die Funktionalitäten im Administratorkontext verwendet werden. In Kombination mit einer weiteren Schwachstelle (siehe folgende Schwachstelle „Remote-Code-Execution“) ist es möglich, Code auf dem unterliegenden System auszuführen. Dies wurde daher als kritisch bewertet.
- **Remote-Code-Execution:** Diese Schwachstelle trat in zwei Produkten auf und wurde ebenfalls als kritisch bewertet, da es einer Angreiferin bzw. einem Angreifer über gefährliche Funktionen in Vorlagen möglich war, eigenen Code in die Anwendung einzuschleusen, über diesen dann Systembefehle ausgeführt werden konnten. In beiden Fällen war dies jedoch ausschließlich durch die Rolle als Administrator ausnutzbar.
- **Unsicherer Dateiupload:** Ebenfalls als kritisch bewertet wurde in einem Fall ein unsicherer Dateiupload. In diesem Fall war es möglich Code über den Upload von schadhaften Dateien auf dem unterliegenden System auszuführen, was potenziell zur Übernahme des Webservers führen kann. Auch diese Schwachstelle war lediglich in der Rolle als Administrators ausnutzbar, hatte jedoch in der Auswirkung gravierende Folgen.

- **Persistentes Cross-Site Scripting (XSS):** Während der Prüfungen identifizierte das Projektteam insgesamt drei Schwachstellen, die im Zusammenhang mit persistentem Cross-Site-Scripting stehen. Ein Cross-Site-Scripting beschreibt einen Angriff auf eine Webanwendung, der auf fehlerhafte Validierung von Ein- und Ausgabedaten zurückzuführen ist. Über die Schwachstelle kann es Angreiferinnen und Angreifern gelingen, eigenen Code in der Anwendung auszuführen. In zwei Fällen wurde dies mit mittlerem Risikograd bewertet. In einem Fall wurde die Schwachstelle jedoch als kritisch bewertet. Dies ist darauf zurückzuführen, dass die Verwundbarkeit im Administratoren-Interface identifiziert wurde. In Kombination mit einer anderen Schwachstelle, bei der eine anonyme Angreiferin bzw. ein anonymer Angreifer eine angemeldete Administratorin oder einen angemeldeten Administrator dazu bringen musste, einen manipulierten Link zu klicken, könnte diese Schwachstelle dazu führen, dass im Administratorenkontext schadhafter Code innerhalb der Anwendung ausgeführt wurde. Im schlimmsten Fall hätte dies bedeutet, dass Administratorenkonten übernommen werden konnten.

Zuordnung zur OWASP Top 10

Die OWASP Top 10[15] ist eine Liste der größten Risiken von Webanwendungen. Sie stellt ein Ranking dar und wird in regelmäßigen Abständen durch die Non-Profit-Organisation OWASP veröffentlicht. In der OWASP Top 10 ist für jede Kategorie jeweils eine Beschreibung des Risikos, diverse Beispiele und exemplarische Angriffsvektoren enthalten. Weiterhin sind Empfehlung hinterlegt, um das Auftreten von Schwachstellen dieser Art zu verhindern. Das Projektteam ordnete die identifizierten Schwachstellen entsprechend ihres Risikos den OWASP Top 10 zu.

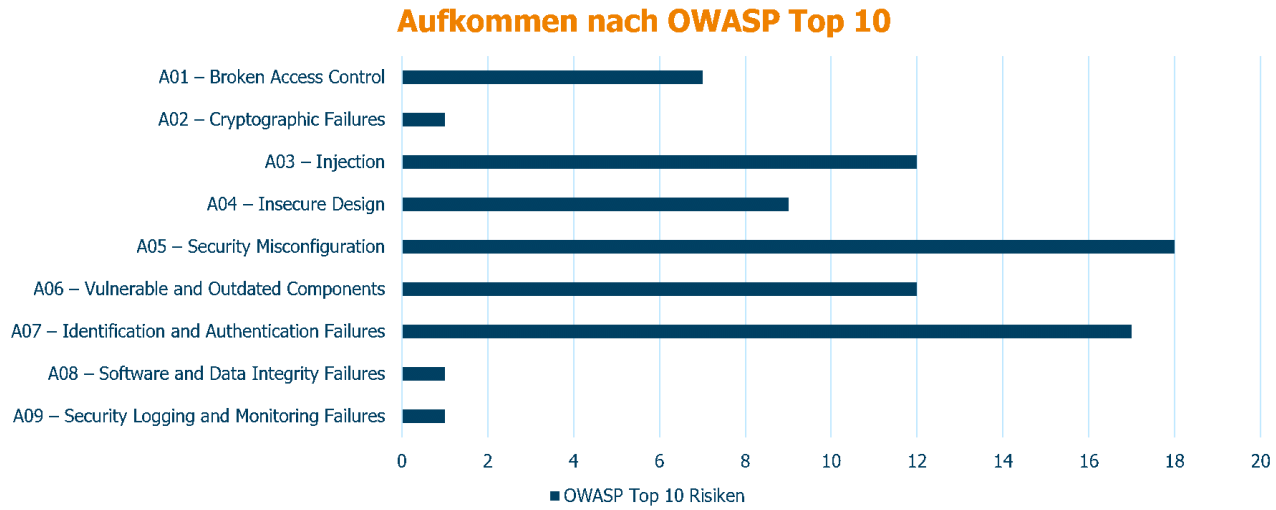


Abbildung 4 Aufkommen der Schwachstellen nach OWASP Top 10

Am häufigsten konnten Schwachstellen in der Kategorie *Security Misconfiguration* angetroffen werden. Anwendungen sind verwundbar gegenüber dieser Kategorie, wenn beispielsweise die Anwendung nicht ausreichend gehärtet wurde, unnötige Accounts oder Berechtigungen vergeben wurden oder die Anwendung selbst oder verwendete *Frameworks* nicht sicher konfiguriert wurden. Insgesamt 18 Schwachstellen, verteilt auf alle Produkte, konnten im Kontext dieser Kategorie gefunden werden.

Am zweithäufigsten traten Schwachstellen in der Kategorie *Identification and Authentication Failures* auf. In diese Kategorie fallen Brute-Force-Verwundbarkeiten der Anmeldemaske, unzureichende Passwortrichtlinien und Schwachstellen im Session Management. Hier konnten insgesamt 17 Schwachstellen über alle geprüften Produkte hinweg identifiziert werden.

Jeweils zwölf Mal traten über alle geprüften Shop-Softwareprodukte hinweg Schwachstellen in den Kategorien *Injection* und *Vulnerable and Outdated Components* auf. *Injection* Schwachstellen sind auf Verwundbarkeiten zurückzuführen, bei denen es einer Angreiferin bzw. einem Angreifer gelingt, eigenen

[15] https://owasp.org/www-project-top-ten/

Code in der Anwendung einzuschleusen. Die Kategorie der verwundbaren und nicht mehr unterstützten Softwarekomponenten beinhaltet alle Schwachstellen, die auf den Einsatz von verwundbarer Software oder nicht mehr unterstützte Software zurückzuführen sind.

Risikograde der einzelnen Schwachstellen

Schwachstellen, die das Projektteam während der Analyse identifizierte, wurden nach der Metrik des CVSS in verschiedene Risikograde eingestuft.

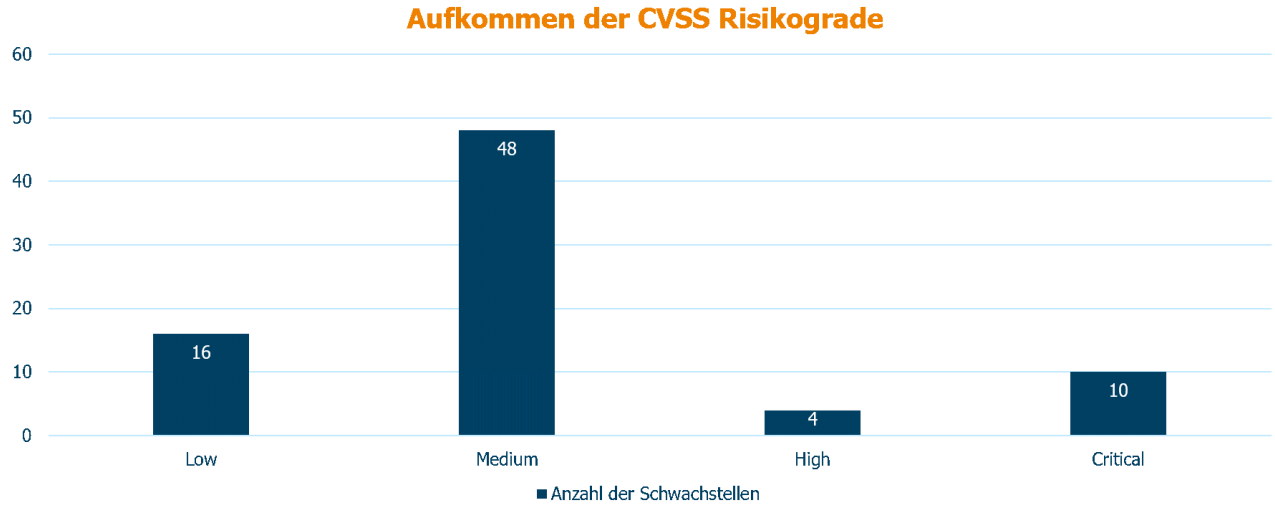


Abbildung 5: Aufteilung der Schwachstellen nach Risikograden

Die meisten der 78 identifizierten Schwachstellen wiesen einen mittleren Risikograd auf. Die am häufigsten (neun Mal) identifizierte Schwachstelle mit mittlerem Risikograd bezieht sich auf eine schlechte, nicht konfigurierbare Passwortrichtlinie. Insgesamt sieben Mal und somit am zweithäufigsten wurden JavaScript-Bibliotheken identifiziert, die Verwundbarkeiten gegenüber bekannten Schwachstellen aufwiesen.

Schwachstellen mit niedrigem Risikograd wurden insgesamt 16-mal gefunden. Alle Produkte waren von der Verwundbarkeit der Übertragung von sensiblen Informationen aus Formularfeldern an Dritte betroffen. Diese Schwachstelle stellte daher die am häufigsten gefundene Schwachstelle mit niedrigem Risikograd dar. Die zweithäufigste Schwachstelle in dieser Kategorie bezieht sich auf die Sicherheitseigenschaften des Cookies, welches die Shop-Software ausliefert. Das Secure-Merkmal war in diesen Fällen nicht gesetzt, so dass das Cookie potenziell auch über einen unverschlüsselten Kanal versendet werden könnte. Dies würde einer Angreiferin oder einem Angreifer, die bzw. der Daten passiv mitlesen kann, erlauben, das übertragene Cookie mitzulesen und so unberechtigten Zugang zur Session einer Benutzerin oder eines Benutzers zu erlangen.

Insgesamt zehn Schwachstellen mit einem kritischen Risikograd wurden über alle geprüften Produkte hinweg gefunden. Der hohe Wert ist drauf zurückzuführen, dass vermehrt Software im Einsatz war, die das offizielle EOL bereits überschritten hat (fünf Mal). Alle weiteren kritischen Schwachstellen traten jeweils nur einmalig auf und wurden bereits in den vorherigen Absätzen erläutert.

Schwachstellen eines hohen Risikograde wurden am wenigsten angetroffen. Insgesamt wurden hierbei vier Verwundbarkeiten identifiziert, die alle jeweils einmalig auftraten. Eine Verwundbarkeit bezieht sich hierbei darauf, dass die Datenbank Zugangsdaten in Log-Dateien erfasst. Nach der Installation waren diese Log-Dateien im Klartext abspeichert und öffentlich zugänglich. Einer anonymen Angreiferin oder einem Angreifer wäre es so möglich auf diese Zugangsdaten zuzugreifen und Zugang zu allen Daten in der Datenbank zu erhalten.

3.3.2 CVD-Prozess

Das BSI hat die gewonnenen Erkenntnisse der Schwachstellenanalysen an die jeweiligen Hersteller übermittelt. Ziel des CVD-Prozesses war es, den Herstellern infolge der identifizierten Schwachstellen den Schutzbedarf der Verbraucherdaten zu verdeutlich sowie den Bedarf an einer Verbesserung der IT-Sicherheitsmaßnahmen zu vermitteln. Wichtig war dem Projektteam dabei, dass die Hersteller jeweils eine nachvollziehbare Dokumentation und ausreichend Zeit für eine Reaktion und die Bereitstellung eines Patches erhalten. Dies sollte sicherstellen, dass das IT-Sicherheitsniveau der jeweiligen Shop-Software nachhaltig verbessert werden konnte und keine neuen Schwachstellen durch die Anpassungen in die Anwendung eingebracht wurden. Hierfür war es essentiell, dass das Projektteam im Rahmen des CVD-Prozesses für die Hersteller ansprechbar war, wenn Schwachstellen nachgestellt werden mussten oder es Rücksprachbedarf über Möglichkeiten zur Behebung einzelner Schwachstellen gab.

Ein erfolgreicher CVD-Prozess setzt darüber hinaus einen verantwortungsbewussten und effizienten Reaktionsprozess seitens der Hersteller voraus, um das von einer Schwachstelle ausgehende Schadensszenario und das daraus resultierende Schadensrisiko zu reduzieren. Im Rahmen einer solchen Diskussion ist es gängig, dass Hersteller Schwachstellen anders bewerten. Hersteller haben in der Regel ein umfangreiches Hintergrundwissen über die genaue Funktionsweise der Anwendung. Dadurch können im Zweifel bestimmte Auswirkungen im konkreten Fall erfolgreich mitigiert werden. Sicherheitsexpertinnen und -experten haben einen anderen, prinzipiellen Blickwinkel auf die Thematik. Sie bewerten eine Schwachstelle stets mit Blick auf den „worst case possible“. Bei der Bewertung der gefundenen Schwachstellen sollten daher in jedem Fall beide Perspektiven betrachtet werden und ein Austausch zwischen Sicherheitsexpertinnen und -experten sowie Herstellern ermöglicht werden.

Während des CVD-Prozesses wurden beispielsweise einige Schwachstellen durch die Hersteller entkräftet, da die Schwachstellen im Testsystem des Testteams zwar vorhanden waren, diese aber durch eine entsprechend sichere Konfiguration des Produkts behoben werden konnten. Letztlich verblieb eine unzureichende Anleitung als Kritikpunkt, da dadurch eine Konfiguration im Sinne von *Security per default* nicht gegeben war.

Zum Zeitpunkt der Veröffentlichung dieses Abschlussberichts war der CVD-Prozess noch nicht abgeschlossen. Die Mehrheit der Hersteller (acht von zehn) hat auf die identifizierten Schwachstellen reagiert und diese validiert. In einigen Fällen konnten Patches in Aussicht gestellt werden, so dass der Austausch im Rahmen des CVD-Prozesses zusammenfassend als positiv zu bewerten ist.

4 Repräsentative Bevölkerungsumfrage

4.1 Methodisches Vorgehen

4.1.1 Qualitative Vorphase

Vor der repräsentativen Verbraucherbefragung wurden 15 Interviews mit jeweils einer Länge von 90 Minuten durchgeführt. Diese fanden im Mai und Juni 2022 statt, elf davon mit Expertinnen und Experten zum Thema Onlineshopping:

- fünf Interviews mit technisch versierten Experten mit Arbeitsschwerpunkten wie Programmierung, Entwicklung, Datenschutz oder redaktionelle Tätigkeiten.
- vier Interviews mit Expertinnen und Experten mit einem fundierten Blick auf Verbraucherinnen und Verbraucher wie z. B. Verantwortliche aus Verbraucherzentralen und Forschungseinrichtungen,
- zwei Interviews mit Shop-Betreibern.

Mit Blick auf die Entwicklung des Fragebogens für die Verbraucherbefragung wurden zudem vier Interviews mit sogenannten Heavy-Shopperinnen und –Shoppern[16] durchgeführt.

4.1.1.1 Planung und Durchführung

Die Expertinnen und Experten sollten ihre Bewertungen zu unterschiedlichen Shopsystemen bzw. Anforderungen an deren IT-Sicherheit diskutieren sowie ihre Wahrnehmung von Datenleak-Vorfällen erläutern. Ihr professioneller Blick auf die Situation der Verbraucherinnen und Verbraucher beim Onlineshopping half, den Ergebnissen der Verbraucherbefragung eine weitere Perspektive an die Seite zu stellen.

Die Interviews mit den Heavy-Shopperinnen und -Shoppern dienten in erster Linie dazu, die Denkweise von Verbraucherinnen und Verbrauchern besser verstehen zu lernen. Dies stellte sicher, dass für die anschließende Verbraucherbefragung alle Befindlichkeiten und Überlegungen der Verbraucherinnen und Verbraucher offengelegt waren und in den Fragebogen als Statements und Fragen eingingen.

4.1.1.2 Ableitungen für den Fragebogen

Aus den Interviews mit den Heavy-Shopperinnen und -Shoppern konnten. zu folgenden Themen Statements abgeleitet werden:

- Verschiedene Arten des Verständnisses von Datensicherheit
- Vervollständigung von Einstellungen zum Umgang mit Risiken beim Onlineshopping
- Statements zu verschiedenen Arten von Schutzmaßnahmen

Dies sollte für den Fragebogen die Erhebung eines möglichst vollständigen Bildes der Verbraucherperspektive sicherstellen. Darüber hinaus konnten aufbauend auf den Ergebnissen der qualitativen Verbraucher- und Experteninterviews folgende Thesen aufgestellt werden:

- Verbraucherinnen und Verbraucher sind sich der Risiken beim Onlineshopping in Bezug auf die Datensicherheit nicht bewusst.
- Verbraucherinnen und Verbraucher erwarten, dass Onlineshops sich um die Sicherheit ihrer persönlichen Daten kümmern.

[16] Heavy-Shopperinnen und -Shopper sind hier definiert über mindestens zwei Online-Einkäufe pro Woche und der Nutzung verschiedener Onlineshops zum Einkaufen, nicht nur ein oder zwei großer Plattformen.

- Schutz vor finanziellem Schaden ist für Verbraucherinnen und Verbraucher das einzig Relevante.
- Je größer die Onlineshopping-Plattform, desto mehr Vertrauen haben die Verbraucherinnen und Verbraucher.
- Verbraucherinnen und Verbraucher wollen ein Kennzeichen für sichere Onlineshops.
- Wenn es zu einem Datenleak kommt, wissen Verbraucherinnen und Verbraucher nicht, was dann zu tun ist, und resignieren.
- Verbraucherinnen und Verbraucher sind sich der Auswirkungen von Datenleaks nicht bewusst.
- Je häufiger Verbraucherinnen und Verbraucher mit Datenleaks konfrontiert sind, desto mehr beschäftigen sie sich mit Schutzmaßnahmen.

Die Überprüfung dieser Thesen erfolgt im Rahmen der quantitativen Befragung in Kapitel 5.1.2

4.1.2 Quantitative Hauptbefragung

Der Fragebogen wurde auf Basis der Ergebnisse der qualitativen Untersuchung entwickelt. Dabei wirkten die Kolleginnen und Kollegen, die an der qualitativen Erhebung beteiligt waren, sowie die Verantwortlichen des BSI mit.

Die Studie wurde im sogenannten Mixed-Method-Verfahren durchgeführt. Hierfür wurde ein Drittel der Befragten im Rahmen eines Online-Interviews (CAWI) um Teilnahme gebeten und zwei Drittel wurden telefonisch (CATI) auf Basis einer Zufallsauswahl befragt.

Für die Qualitätssicherung des Fragebogens und zur Überprüfung der Fragebogendauer sowie der Dramaturgie des Fragebogens fand vom 18.08.2022 bis zum 20.08.2022 ein Pretest mit 53 Befragten (davon 43 CATI, 10 CAWI) statt. Auf Grundlage der Pretestergebnisse wurden Inhalte zusammengefasst oder angepasst und Fragen gestrichen.

Nach der Auswertung der Pretestergebnisse umfasste der Fragebogen folgende Inhalte:

- Internetnutzung
- Nutzung und Häufigkeit von Onlineshopping sowie verschiedener Endgeräte, digitaler Dienste und Anwendungen
- Gründe gegen Onlineshopping
- Bedenken im Hinblick auf Onlineshopping
- Verständnis, Bekanntheit und Interesse von Datensicherheit
- Sorge und Erfahrung bezüglich Datensicherheitsvorfällen
- Einstellung zu und Umgang mit Risiken, Selbstwirksamkeit
- Bekanntheit und Anwenden von Schutzmaßnahmen
- Informiertheit bzgl. Datensicherheit, Bekanntheit des BSI
- Soziodemographie (Alter, Geschlecht, Haushaltsgröße, Kinder, Bildung, Einkommen, Berufstätigkeit, Region, etc.)

Der vollständige Fragebogen mit genauer Frageformulierung ist im Anhang zu finden.

4.2 Durchführung

4.2.1 Zielgruppen-Beschreibung

Die Grundgesamtheit der Untersuchung war die deutschsprachige Wohnbevölkerung im Alter von 16-74 Jahren, die in den letzten zwölf Monaten das Internet genutzt hat. Für diese galt es, repräsentative Erkenntnisse in Bezug auf das Risikobewusstsein, die Urteilsfähigkeit und die Lösungskompetenz im Zusammenhang mit Datenleak-Vorfällen beim Onlineshopping zu ermitteln.

4.2.2 Erhebungsmethode

CATI-Interviews sind, in Abgrenzung zu Online-Interviews, aufgrund der theoretischen Vollständigkeit der Auswahlgrundlage besser geeignet, bevölkerungsrepräsentative Ergebnisse zu erzielen, vor allem dann, wenn eine Zufallsauswahl aus einer kombinierten Festnetz- und Mobilfunkstichprobe (ADM Dual Frame) zum Einsatz kommt. Dadurch werden auch mobilere Personengruppen oder Personen, die über keinen Festnetzanschluss verfügen, erreicht. Da aber die Teilnahmerate an telefonischen Interviews in den letzten Jahren gesunken ist, und vor allem jüngere Personen schwerer für telefonische Umfragen zu gewinnen sind, kann eine gezielte Integration von Online-Interviews im Rahmen eines Mixed-Method-Ansatzes den Coverage-Problemen[17] methodisch entgegenwirken. Für das vorliegende Forschungsvorhaben wurde entschieden, jeweils in beiden Erhebungsansätzen die adressierte Grundgesamtheit abzubilden.

Um ein weitestgehend gleiches Erhebungsinstrument einzusetzen, ist beim Einsatz von unterschiedlichen Erhebungsmethoden die Orientierung am schwächeren Modus ausschlaggebend. Im vorliegenden Fall handelt es sich dabei um die selbstadministrierten Online-Interviews.

Mit dem Ziel generalisierbare, repräsentative Ergebnisse zu ermitteln und damit auch Aussagen über Personengruppen treffen zu können, die das Internet seltener und mit größerer Vorsicht nutzen, wurde ein Mischungsverhältnis der beiden Erhebungsarten festgelegt. Der größere Anteil der Interviews fand daher auf Basis persönlicher, telefonischer Interviews mittels Zufallsauswahl statt. Des Weiteren kam ein Panel zum Einsatz, welches ausschließlich offline rekrutiert wurde (GIMpulse). Die Rekrutierungsart dieses Panels gewährleistet, dass Selbstselektionseffekte, wie sie z.B. bei Anwerbungen über Websites auftreten können, weitestgehend ausgeschlossen werden. Das Stichprobenkonzept berücksichtigte für die Erhebung 63 Prozent CATI-Interviews (60 Prozent Festnetz, 40 Prozent Mobilfunk gemäß ADM-Empfehlung) und 37 Prozent Online-Interviews. Mit diesem Vorgehen wird sowohl einer Verzerrung der Ergebnisse, die durch die Korrelation von Untersuchungsgegenstand und -methode hervorgerufen werden kann, wie auch einer Überzeichnung der Nutzung digitaler Techniken und Angebote vorgebeugt.

Die Studienanlage wird nachfolgend im Überblick beschrieben.

Tabelle 5 Studienüberblick quantitative Befragung

Elemente der Befragung	***CATI-Befragung***	***CAWI-Befragung***
Erhebungszeitraum	Pretest: 18.-20.08.2022 Hauptbefragung: 31.08.2022-24.09.2022	Pretest: 18.-20.08.2022 Hauptbefragung: 07.09.2022-17.09.2022
Grundgesamtheit	Deutschsprachige Wohnbevölkerung im Alter von 16 -74 Jahren, die in den letzten zwölf Monaten das Internet genutzt hat (Hochrechnungsbasis: 57, 046 Millionen)	Deutschsprachige Wohnbevölkerung im Alter von 16 -74 Jahren, die in den letzten zwölf Monaten das Internet genutzt hat (Hochrechnungsbasis: 57, 046 Millionen)

[17] Unter Coverage-Problemen sind in diesem Zusammenhang systematische Fehler bzw. Verzerrungen in der Datenbasis zu verstehen, wenn die im Rahmen einer Befragung erreichte Personengruppe in ihrer Struktur nicht der relevanten Grundgesamtheit entspricht.

Elemente der Befragung	*CATI-Befragung*	*CAWI-Befragung*
Anzahl Interviews Hauptbefragung	642	376
Durchschnittliche Interviewlänge	Mittelwert: 23,5 Minuten	Mittelwert: 13,9 Minuten
Auswahlrahmen	ADM Dual Frame Mastersample	GIMPulse – Offline rekrutiertes Panel
Feldarbeit	Durchführung: GIM DiCom	Durchführung: GIM DiCom
Datenaufbereitung	Abschließende Plausibilitätskontrolle, Gewichtung, Kontrolle der Repräsentativität	Abschließende Plausibilitätskontrolle, Datenbereinigung, Gewichtung, Kontrolle der Repräsentativität
Auswertung	Tabellierung, deskriptive, statistische und multivariate Analysen. Die Auswertung und Analyse erfolgt auf Basis der Gesamtdaten beider Erhebungsmethoden.	Tabellierung, deskriptive, statistische und multivariate Analysen. Die Auswertung und Analyse erfolgt auf Basis der Gesamtdaten beider Erhebungsmethoden.

4.2.3 CATI

Um einen bevölkerungsrepräsentativen Querschnitt der deutschsprachigen Wohnbevölkerung im Alter von 16 -74 Jahren zu befragen, die in den letzten zwölf Monaten das Internet genutzt hat, wurde der Anteil der Telefoninterviews auf Basis einer Dual Frame-Stichprobe durchgeführt.

Dual-Frame-Auswahlrahmen

Für die Durchführung bevölkerungsrepräsentativer Studien wurde das ADM-Stichprobensystem für Telefonbefragungen genutzt: Der Auswahlrahmen basiert auf den von der Bundesnetzagentur jährlich zur Nutzung bereitgestellten Nummernbereichen. Diese Nummernbereiche umfassen prinzipiell alle in der Bundesrepublik Deutschland nutzbaren Telefonnummern – auch Mobiltelefonnummern. Um der Zunahme der Mobilfunknutzung Rechnung zu tragen, wurde für die Untersuchung eine Dual-Frame-Verteilung von 60 zu 40 (Festnetz zu Mobil) berücksichtigt. Beim Dual-Frame-Design sind die unterschiedlichen Auswahlmethoden der Zielperson im Haushalt zu berücksichtigen: Während in der im vorliegenden Bericht betrachteten Studie bei der Festnetzstichprobe eine Zielperson im Haushalt durch das Last-Birthday-Verfahren ausgewählt wird, gilt in der Mobilfunkstichprobe die Person, die den Anruf auf dem Handy entgegennimmt, als Zielperson.

Um Ungleichheiten in den Auswahlchancen und designbedingte Schiefen auszugleichen, wurden die Daten einer Gewichtung unterzogen, bei der beide Teilstichproben sowohl in eine Design- als auch in eine Strukturgewichtung einbezogen wurden. Als Referenzdaten wurde der Gewichtung die Verteilung des aktuellen Mikrozensus[18] zugrunde gelegt. Aufgrund der aktuellen Umstellung der Mikrozensus-Erhebung sowie der abgebildeten Grundgesamtheit der Internetnutzer wurde darüber hinaus die Verteilung der ma Audio 2021 (Grundlagenstudie der Medienforschung mit n=67.054 Interviews), die ihrerseits gemäß der Amtlichen Statistik gewichtet wurde, zugrunde gelegt. Insgesamt wurden folgende Variablen und Variablenausprägungen für die deutschsprachige Wohnbevölkerung im Alter von 16-74 Jahren, die das

[18] Statistisches Bundesamt. 2021. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien (Mikrozensus-Unterstichprobe zur Internetnutzung). Fachserie 15 Reihe 4, 14-16.

Internet nutzt, in die Gewichtung einbezogen: Alter, Geschlecht, Westdeutschland, Ostdeutschland, Bildung, Haushaltsgröße, BIK-Regionsgröße (Siebener-Einteilung)[19] und Bundesland.

Feldarbeit CATI-Befragung

Bei den Interviews kamen folgende Qualitätsstandards zum Einsatz:

- Computergestützte Telefoninterviews mit automatisiertem Samplemanagementsystem (SMS).
- Intelligentes Steuerungskonzept zur Verteilung der Anrufe und Abarbeitung des Kontaktschemas pro Rufnummer über verschiedene Tageszeiten und Wochentage für eine bestmögliche Ausschöpfung der Stichprobe.
- Einsatz von festangestellten, erfahrenen, muttersprachlichen Interviewerinnen und Interviewern.
- Kontinuierliche Betreuung der Interviewerinnen und Interviewer durch permanent anwesende Supervisorinnen und Supervisoren.
- Projektspezifische Schulung.

4.2.4 CAWI

Für die Online-Interviews wurde auf das GIM-Online-Panel zurückgegriffen. Dieses Panel ist frei von Selbstselektionseffekten und bildet die Grundlage für repräsentative Erhebungen. Die Rekrutierung basiert auf CATI-Interviews, Face-to-Face-Interviews, sowie postalischen Rekrutierungen. Der Einsatz dieser drei Methoden gleicht Schwächen einzelner Modi aus.

Feldarbeit Online-Befragung

Bei den Online-Interviews kamen folgende Qualitätsstandards zum Einsatz:

- Die Befragten wurden per E-Mail und personalisiertem Link zur Befragung eingeladen.
- Regionale und demographische Vorschichtung des Panels und zufallsbasierte Ziehung pro Zelle, um eine Streuung auch über verschiedene Teilnehmertypen zu erzielen.
- Streuung der Einladung und Versand an verschiedenen Werk- und Wochenendtagen.
- Die Panellisten erhielten für die Teilnahme ein Incentive.

4.2.5 Stichprobe und Gewichtung

Da es im Laufe der Erhebung zu Interviewausfällen kommen kann, die eine Abweichung der Verteilung zur Folge haben kann, wurden die Erhebungsdaten im Vorfeld der Ergebnisanalysen einer Gewichtung unterzogen. Diese orientierte sich an dem durch den ADM für Dual Frame Stichproben empfohlenen Gewichtungsmodell. Hierfür werden die erhobenen Daten durch eine Designgewichtung miteinander kombiniert, in dem die Inklusionswahrscheinlichkeiten korrigiert werden.

Die Gewichtung erfolgte dann in drei Schritten:

1. Transformation:
   Zunächst wurden die unterschiedlichen Auswahlchancen einer einzelnen Person, je nach Modus (Festnetz oder Mobilfunk), in die Stichprobe zu gelangen, bereinigt. Bei der Festnetzstichprobe wurde dazu die Anzahl der Festnetznummern, unter der die befragte Person zu erreichen ist (Haushaltstransformation) und die Anzahl der Personen im Alter zwischen 16-74 Jahre innerhalb eines Haushaltes (Personentransformation) ermittelt. Bei der Mobilfunkstichprobe wurde die Anzahl der Mobilfunknummern, unter der die Person zu erreichen ist, ermittelt. Größeren Wahrscheinlichkeiten in

[19] Für statistische Analysen wird häufig eine Einteilung von Wohnorten in sieben Größenklassen verwendet. Das BIK-Ortsgrößen- oder Gemeindegrößensystem sind eine bundesweite räumliche Gliederungssystematik, die die Stadt-Umland-Beziehungen auf Gemeindeebene für Ballungsräume, Stadtregionen, Mittel- und Unterzentren darstellt.

eine Stichprobe zu gelangen, wurde ein entsprechendes niedrigeres Transformationsgewicht zugeordnet, kleineren ein entsprechend höheres.

2. Zusammenführung der Teilstichproben (Festnetzstichprobe, Mobilfunkstichprobe, Online-Stichprobe): Im nächsten Schritt wurden die Teilstichproben zu einer Gesamtstichprobe zusammengeführt und somit in das korrekte Verhältnis gesetzt. Danach war für alle Befragten der Netto-Gesamtstichprobe die Auswahlchance durch die Gewichtung gleichgesetzt.
3. Redressment:
   Anschließend wurde die Struktur der Stichprobe hinsichtlich soziodemographischer Merkmale an die Struktur der Grundgesamtheit nach Amtlicher Statistik angeglichen. Da Teilnehmerinnen und Teilnehmer in einem Online-Panel in der Regel höhere Internetnutzungsfrequenzen aufweisen und auch in Bezug auf ihr Onlineshoppingverhalten vom Durchschnitt der Bevölkerung abweichen können, wurde für die Onlinestichprobe ebenfalls eine Transformationsgewichtung durchgeführt. Hierbei wurde die Einkaufsfrequenz im Internet in der Onlinestichprobe an die der CATI-Stichprobe angeglichen. Für die CATI-Stichprobe wurde im Vorfeld die oben beschriebene Transformation und eine Gewichtung der soziodemographischen Variablen entsprechend der Referenzdaten durchgeführt. Den abschließenden Schritt bildete das oben beschriebene Redressment nach der Zusammenführung aller Teilstichproben.

Die für die Gewichtung erforderlichen Konventionen wie z. B. die Zuordnung von Missings wurden im Datensatz beschrieben und dokumentiert.

4.2.6 Datenbereinigung

Im Feldverlauf wurden kontinuierlich folgende Kontrollen und Datenbereinigungen bei den Online-Interviews durchgeführt:

- Speeder: Als realistische Befragungszeit betrachtet die Forschungspraxis die 50 Prozent Intervallgrenze unterhalb des Medians, wobei die Basis der Berechnung der Zeitstempel ist. Nach nochmaliger Prüfung erfolgt ein Ausschluss dieser Fälle. Im Datensatz der vorliegenden Studie wurden sechs Fälle identifiziert und ausgeschlossen, die unterhalb der definierten Grenze lagen.
- Flatliner: Befragte, die über mehrere Itembatterien keine Varianz aufweisen. Konkret wurden hier diejenigen Befragten ausgeschlossen, die in Frage Q5 (Bedenken beim Onlineshopping gestützt) und Q13 (Relation Gefahren im Internet allgemein vs. Datensicherheit) jeweils durchgängig über alle Items hinweg denselben Wert angegeben haben. Dies waren acht Fälle, die entsprechend aus der Analyse ausgeschlossen wurden.
- Stichproben bei offenen Texten: Hier ergaben sich keine Auffälligkeiten.

Alle Prüfungen wurden im Kontext betrachtet, da z. B. wenig Varianz bei einer Statementbatterie allein durchaus plausibel sein kann, in der Kombination mit einer unterdurchschnittlichen Befragungszeit beispielsweise aber ein Hinweis auf ein Durchklicken des Fragebogens sein kann. Insgesamt wurden so 14 Fälle der Online-Befragung identifiziert und aus der Analyse ausgeschlossen.

Im Sinne der Plausibilisierung wurden als weitere Prüfung die offenen Nennungen in Frage Q15 (Reaktionen auf Vorfall in Bezug auf Datensicherheit) auf Zuordenbarkeit in bereits vorhandene Kategorien hin gesichtet und entsprechend vercodet.

4.3 Ergebnisse der Bevölkerungsumfrage

Meldungen zu Datenleak-Vorfällen, also dem Diebstahl bzw. dem Offenlegen von Daten, die nicht für die Öffentlichkeit bestimmt oder geeignet sind, sind für das BSI keine Seltenheit.

Um Wissenstand und Relevanz des Themas Datensicherheit beim Onlineshopping in seiner Breite zu beleuchten und um Bereiche zu identifizieren, die durch Kommunikationsmaßnahmen verbessert werden können, wurde eine repräsentative Untersuchung durchgeführt. Hier fließen auch die Erkenntnisse der im Vorfeld durchgeführten qualitativen Gespräche ein. Im Fokus standen die Fragen:

- Wie nehmen Verbraucherinnen und Verbraucher Risiken beim Onlineshopping wahr und welche Relevanz hat das Thema für sie?
- Wie bewerten Verbraucherinnen und Verbraucher konkrete Risiken, die sie wahrnehmen?
- Welche Schutzmaßnahmen kommen zur Eindämmung des Risikos zur Anwendung?
- Welche Lösungsstrategien entwickeln Verbraucherinnen und Verbraucher beim Thema Datensicherheit beim Onlineshopping?
- Welche Unterschiede lassen sich in der Bevölkerung identifizieren?

Für die Reproduzierbarkeit und weiterführende Analyse der quantitativen Befragung stehen die bereinigten Einzeldaten sowie das entsprechende Codebook unter https://www.bsi.bund.de/dok/1084596 bereit.

4.3.1 Kaufverhalten, Zugang und Barrieren beim Onlineshopping

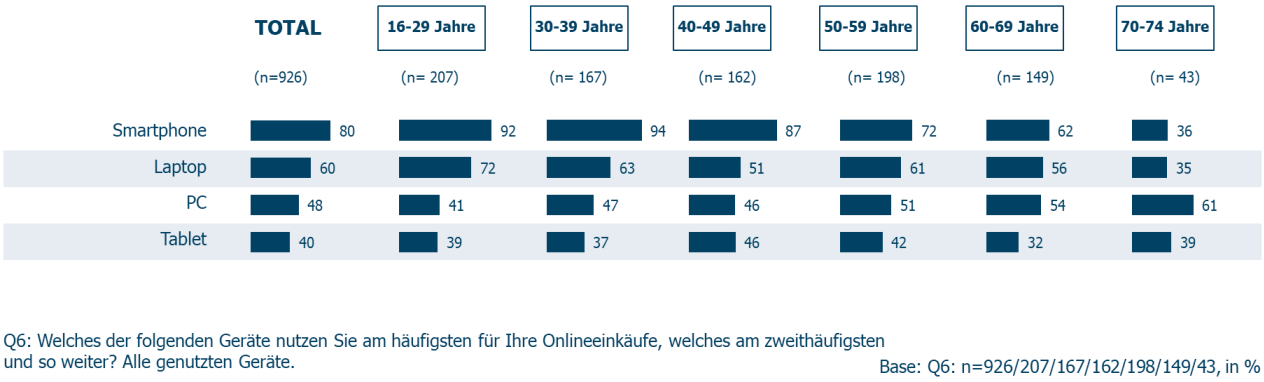
Zunächst wurden folgende Fragestellungen im Zusammenhang mit der Nutzung von Onlineshopping betrachtet:

- Wer kauft in welcher Intensität online ein?
- Welche Geräte kommen dabei zum Einsatz?
- Welche Gründe halten die Verbraucherinnen und Verbraucher vom Onlineshopping ab - stehen Unsicherheiten im Zusammenhang mit der Datensicherheit und dem Datenschutz im Vordergrund oder sind es andere Gründe?
- Wie unterscheiden sich Verbrauchergewohnheiten - liegen unterschiedliche Gewohnheiten beim Onlineshopping z. B. in Bezug auf Lebensphasen oder formalen Bildungsstand vor?

91 Prozent aller Befragten gaben an, zumindest gelegentlich bei Onlineshops einzukaufen. Demgegenüber stehen neun Prozent, die dies nicht tun. Der häufigste Grund dafür, dies nicht zu tun, ist für Befragte, die nicht im Internet einkaufen, dass sie sich die entsprechenden Produkte gerne im Geschäft ansehen und sie dort direkt mitnehmen können (86 Prozent). Außerdem wollen sie den lokalen Einzelhandel unterstützen (72 Prozent).

Die Mehrheit derjenigen, die zumindest gelegentlich Onlineshops nutzt, kauft ein- oder mehrmals pro Monat im Internet ein (55 Prozent).

Gefragt nach dem Gerät, das grundsätzlich von Verbraucherinnen und Verbrauchern für den Onlineeinkauf verwendet wird, zeigt sich, dass der Alltagsbegleiter Smartphone mit 80 Prozent für die deutliche Mehrheit der Befragten das Gerät der Wahl ist. Sechs von zehn Befragten wählen den Laptop, um Waren und Dienstleistungen online zu kaufen. Das Tablet nutzen nur ca. 40 Prozent, den PC hingegen knapp die Hälfte der Befragten. Gerade bei der PC-Nutzung zeigen sich geschlechtsspezifische Unterschiede: Mit 56 Prozent sind es vor allem Männer, die einen PC für das Einkaufen verwenden (Frauen 40 Prozent). Bei der Betrachtung der Altersgruppen fällt auf, dass das Smartphone vor allem das Gerät der Jüngeren ist: über 90 Prozent der 16-39-Jährigen nutzen es zum Onlineshopping.



Q6: Welches der folgenden Geräte nutzen Sie am häufigsten für Ihre Onlineeinkäufe, welches am zweithäufigsten und so weiter? Alle genutzten Geräte.

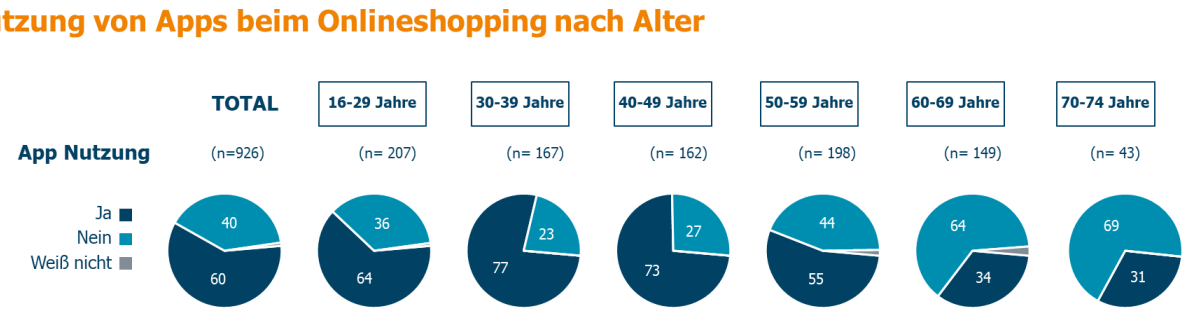
Base: Q6: n=926/207/167/162/198/149/43, in %

Abbildung 6 Nutzung von Endgeräten beim Onlineshopping nach Alter

Aber auch Unterschiede mit Blick auf das Interesse am Thema Datensicherheit beim Onlineshopping sind zu verzeichnen: Die Hälfte derjenigen, die zumindest gelegentlich in Onlineshops einkaufen und sich sehr für das Thema Datensicherheit interessieren, nutzt den PC (53 Prozent Interessierte vs. 42 Prozent weniger Interessierte). Hingegen nutzen Personen, die sich nur etwas für das Thema interessieren, deutlich öfter (86 Prozent) das Smartphone. Darüber scheint der Zugang zum Onlineshopping über das Smartphone besonders niedrigschwellig zu sein und wird vor allem von den Befragten genutzt, die häufig online shoppen (97 Prozent).

Für 60 Prozent der Befragten, die mindestens gelegentlich online einkaufen, findet der Zugang zum Onlineshop für bestimmte Anbieterinnen und Anbieter über eine App statt. Die Altersgruppen unterscheiden sich hierbei klar: Befragte, die zwischen 16 und 59 Jahre alt sind, nutzen eine App jeweils deutlich eher als die 60-74-Jährigen - wobei letzteres auch im Zusammenhang mit dem altersspezifisch niedrigeren Anteil der Smartphone-Nutzung zum Onlineshopping in dieser älteren Altersgruppe zu sehen ist (vgl. Abbildung 6).

Interessant ist an dieser Stelle, dass Personen im Alter von 30-49 Jahren Apps deutlich häufiger nutzen als dies jüngere Personen im Alter von 16-29 Jahren tun (vgl. Abbildung 7).



Q7: Bitte denken Sie einmal an Ihre Onlineeinkäufe oder Onlinebuchungen. Nutzen Sie, wenn auch nur für bestimmte Anbieter, eine sogenannte App für die Bestellungen?

Base: Q7: n=926/207/167/162/198/149/43, in %

Abbildung 7 Nutzung von Apps beim Onlineshopping nach Alter

Mit Blick auf die Einkaufsfrequenz lässt sich feststellen, dass je häufiger Verbraucherinnen und Verbraucher online einkaufen, desto höher liegt auch der Anteil der Personen, die zum Einkaufen eine App verwenden (86 Prozent der Personen, die häufig online einkaufen vs. 39 Prozent derer, die dies selten tun).

Unter Rückgriff auf Ergebnisse der qualitativen Interviews mit Verbraucherinnen und Verbrauchern wird deutlich, dass Einfachheit und Schnelligkeit wichtige Treiber für die Wahl des Zugangs zum Onlineshop per Smartphone und passender App sind, vorwiegend bei jüngeren Zielgruppen, aber mit fortschreitender Digitalisierung zunehmend auch bei Älteren. Aussagen der befragten Expertinnen und Experten ergänzen dies mit ihrer Einschätzung, dass die Sorge um die Datensicherheit beim Onlineshopping gegenüber Vorteilen wie Bequemlichkeit, Schnelligkeit oder Niedrigpreis-Wahrnehmung der Käufe in den Hintergrund trete und von diesen überdeckt würde. Dies fügt sich ins Bild der geringeren Besorgtheit jüngerer Verbraucherinnen und Verbraucher beim Thema Datensicherheit in der Verbraucherbefragung, wie im folgenden Kapitel ausgeführt wird.

Es bietet sich daher an, Kommunikation zum Thema Datensicherheit schwerpunktmäßig auf den Wegen auszuspielen, über die vorwiegend online eingekauft wird. Das Smartphone spielt hier die zentrale Rolle, womit vor allem mobil genutzte Kanäle zum Erreichen relevanter Zielgruppen in den Vordergrund rücken.

Wie zu Beginn des Kapitels dargestellt, kaufen rund neun Prozent der Befragten nicht im Internet ein. Nichtnutzerinnen und -nutzer von Onlineshopping sind vor allem ältere Befragte. Der Anteil liegt bei Personen zwischen 70 und 74 Jahren bei 31 Prozent, im Vergleich dazu liegt er bei den 16-29-Jährigen bei sechs Prozent.

Was sind Gründe, die aus Sicht dieser Befragten gegen Onlineshopping sprechen? Dies ist u.a. der Vorteil, Produkte im Geschäft ansehen und direkt mitnehmen zu können. Die Sorge jedoch davor, dass persönliche Daten beim Onlineshopping nicht sicher sein könnten, belegt bei der Häufigkeit der genannten Gründe lediglich den Rangplatz fünf von zwölf. Von schon einmal gemachten Negativ-Erfahrungen beim Onlineshopping berichtet sogar nur jede zehnte befragte Person, die angibt nicht online einzukaufen. Interessant ist, dass knapp vier von zehn Personen, die nicht online einkaufen, unklar ist, wie genau die Bezahlung im Internet oder wie allgemein der Onlineeinkauf funktioniert (31 Prozent).

4.3.2 Bedenken beim Onlineshopping

Das vorangegangene Kapitel hat gezeigt, dass neun von zehn Befragten zumindest gelegentlich bei Onlineshops einkaufen. Um den Wissensstand in der Bevölkerung hinsichtlich möglicher Gefahren beim Onlineshopping in Bezug auf die Sicherheit ihrer persönlichen Daten im Internet zu ermitteln, wurde die Thematik aus verschiedenen Perspektiven beleuchtet: So wurden zunächst die generellen Bedenken der Verbraucherinnen und Verbraucher im Detail erhoben. Im Verlauf der Befragung wurde das Thema weiter vertieft, die inhaltliche Bedeutung der Datensicherheit beim Onlineshopping aus Sicht der Verbraucherinnen und Verbraucher erfragt und die offizielle Definition des BSI aufgezeigt. Auf dieser Basis wurde der Grad der Besorgnis vor einem Datenmissbrauch und die Einschätzung der Eintrittswahrscheinlichkeit eines Vorfalls im Hinblick auf die Datensicherheit beim Onlineshopping untersucht.

4.3.2.1 Datensicherheit: Unterschiede in Wahrnehmung und Umgang

Haben Verbraucherinnen und Verbraucher selbst Bedenken beim Onlineshopping? Welche Unterschiede in der Bevölkerung lassen sich in Bezug auf die konkreten Bedenken und die Beurteilung der Datensicherheit feststellen?

Insgesamt 68 Prozent der Befragten haben generell Bedenken im Zusammenhang mit Onlineshopping. In Abgrenzung zu der soeben betrachteten Frage nach den generellen Bedenken beim Onlineshopping wird deutlich, dass die konkrete Nennung von möglichen Vorkommnissen zu einer höheren Sensibilität für das Thema Bedenken beim Onlineshopping führt:

- Mit 61 Prozent gibt mehr als die Hälfte aller Befragten an, dass sie Bedenken in Zusammenhang mit dem Weiterreichen ihrer persönlichen Daten haben (Top-2-Box[20]) und etwa die Hälfte aller Befragten hat Bedenken, dass persönliche Daten unrechtmäßig eingesehen oder veröffentlicht werden (Top-2-Box).
- Zudem sind es vor allem diejenigen, die sehr selten online einkaufen, die Bedenken in Zusammenhang mit dem Weiterreichen (Top-2-Box: 75 Prozent) und dem Einsehen oder Veröffentlichen persönlicher Daten (82 Prozent) haben. Interessant ist auch, dass bei hohem Interesse am Thema Datensicherheit der Anteil derer, die sich Sorgen in Bezug auf die genannten Datensicherheitsaspekte machen, höher liegt (Top-2-Box: 66 Prozent Weitereichen pers. Daten bzw. 56 Prozent Einsehen oder Veröffentlichen dieser).
- Etwas mehr als ein Drittel hat Bedenken wegen der ggfs. nicht sicheren Passwortverschlüsselung. Etwas höher liegt der Anteil bei Personen, die sich für das Thema Datensicherheit interessieren (vier von zehn Befragten).
- Ein gutes Drittel hat Bedenken hinsichtlich der tatsächlichen Existenz des Onlineshops.
- Die wenigsten Bedenken bestehen gegenüber der Unversehrtheit der Ware bei Lieferung, (Top-2-Box: 14 Prozent).

Abbildung 8 Bedenken Onlineshopping

Zusammenfassend lässt sich feststellen, dass fast alle Befragten Bedenken rund um das Thema Onlineshopping und Datensicherheit haben – am meisten, wenn es um die persönlichen Daten geht. Vor allem Befragte, die nicht im Internet einkaufen, zeigen sich in fast allen Dimensionen besorgter.

4.3.2.2 Zusammenhänge zwischen dem Grad der Besorgtheit und Kerndimensionen

Wie oben beschrieben, ist sich die Mehrheit der Befragten generell der Gefahren beim Onlineeinkauf bewusst – wenn auch in unterschiedlicher Intensität. Womit der Grad der Besorgtheit zusammenhängt, ist Gegenstand des vorliegenden Kapitels. Der Grad der Besorgtheit wurde anhand einer fünfstufigen Skala abgefragt (1=gar keine Sorgen bis 5=große Sorgen). Mit welchen anderen Variablen hängt nun ein höherer Besorgnisgrad zusammen?

Personen mit einem hohen Besorgnisniveau (Antwort 4 oder 5 auf der fünfstufigen Skala=Top-2-Box) sind Personen, die auch generell Bedenken beim Onlineshopping haben (eher als Personen mit Antwort 1 oder 2 auf der fünfstufigen Skala=Low-2-Box). So haben Personen mit einem hohen Besorgnisniveau Bedenken,:

[20] Mit Hilfe von Top-2-Boxen lassen sich Befragte zusammenfassen, die bei einer Mehrpunkt-Skala die beiden höchsten Antwortoptionen angegeben haben. Analoges gilt für die Low-2-Boxen, bei denen die beiden niedrigsten Antwortoptionen zusammengefasst werden.

- dass die persönlichen Daten weitergereicht werden (Top-2-Box: 87 Prozent mit hohem Besorgnisniveau vs. 28 Prozent mit niedrigem Besorgnisniveau. Die folgenden Prozentangaben beziehen sich jeweils analog auf diese beiden Gruppen hohes bzw. niedriges Besorgnisniveau),
- dass die persönlichen Daten wie Name oder Adresse weitergereicht werden (Top-2-Box: 80 Prozent vs. 35 Prozent).
- dass die persönlichen Daten unrechtmäßig eingesehen oder veröffentlicht werden (Top-2-Box: 75 Prozent vs. 25 Prozent),
- dass es sich nicht um einen tatsächlichen Onlineshop handelt (Top-2-Box: 50 Prozent vs. 23 Prozent),
- dass das Passwort für den Kundenbereich nicht sicher verschlüsselt wird (Top-2-Box: 59 Prozent vs. 13 Prozent),
- dass Ware nicht bzw. falsch oder beschädigt ankommt (Top-2-Box: 21 Prozent vs. 12 Prozent).

Personen mit einem höheren Besorgnisniveau ...

- wünschen sich mehr Orientierung beim Onlineshopping, um die Datensicherheit besser einschätzen zu können. So gaben 84 Prozent der Befragten mit hoher Besorgnis an, dass sie sich ein Siegel von einer unabhängigen dritten Stelle wünschen, dass die Sicherheit beim Onlineshopping bewertet und so Orientierung bei der Auswahl der Onlineshops bietet (im Vergleich zu Personen mit niedrigem Besorgnisniveau (71 Prozent).
- wünschen sich deutlich häufiger ein entsprechendes Siegel von staatlicher Seite im Vergleich zu Personen mit weniger oder keinen Sorgen (Top-2-Box: 77 Prozent vs. 52 Prozent).
- halten es für wahrscheinlicher, dass die persönlichen Daten unrechtmäßig von Dritten eingesehen oder entwendet werden (Top-2-Box: 57 Prozent vs. 16 Prozent),
- haben in der Vergangenheit eher schon einmal negative Erfahrungen mit dem Thema gemacht (35 Prozent vs. 12 Prozent),
- sind generell interessierter an dem Thema Datensicherheit beim Onlineshopping als Personen mit niedrigem Besorgnisniveau (Top-2-Box: 31 Prozent vs. 18 Prozent),
- fühlen sich eher hilfloser gegenüber möglichen Vorfällen beim Thema Datensicherheit im Onlineshopping als Personen mit weniger Sorgen: So lehnen Personen mit hohem Besorgnisniveau die Aussage, man könne beim Onlineshopping selbst dafür sorgen, dass die persönlichen Daten sicher sind, eher ab (Low-2-Box: 37 Prozent vs. 22 Prozent).
- fühlen sich auch von staatlicher Seite weniger geschützt im Hinblick auf Datensicherheit beim Onlineshopping als Personen, die sich keine Sorgen machen (Top-2-Box: 14 Prozent vs. 28 Prozent).

Allerdings zeigen sich keine Zusammenhänge zwischen dem Grad der Besorgtheit und dem Anwenden möglicher konkreter Schutzmaßnahmen. Wohl aber zeigt sich, dass Personen, die sich hinsichtlich der Datensicherheit beim Onlineshopping große Sorgen machen, es generell eher vermeiden, überhaupt im Internet einzukaufen, als Personen, die sich keine bzw. nur wenige Sorgen machen: Zehn Prozent der Befragten mit wenigen bzw. keinen Sorgen kaufen überhaupt nicht im Internet ein– demgegenüber stehen 14 Prozent der Befragten mit großen Sorgen. Seltener als einmal pro Halbjahr kaufen drei Prozent der Befragten mit keinen bzw. wenigen Sorgen im Internet ein, während dies bei den Befragten mit großen Sorgen immerhin 13 Prozent sind.

4.3.2.3 Determinanten der Besorgtheit

Wie im vorangegangenen Kapitel erläutert, sind bivariate Zusammenhänge zwischen dem Grad der Besorgtheit und Variablen wie Interesse am Thema, der Einschätzung einer Schadenswahrscheinlichkeit, negativen Erfahrungen in der Vergangenheit etc. vorhanden. So war nun weiterführend die Frage von Interesse, inwiefern sich der Grad der Besorgtheit in Bezug auf Datensicherheit beim Onlineshopping durch

diese Variablen erklären lässt. Hierfür wurde eine lineare Regression auf Basis der gewichteten Daten gerechnet. Die Daten sind skaliert in die Regression eingegangen. Als Maß für die Erklärungskraft des Modells wird das Bestimmtheitsmaß r^2 herangezogen; dieses nimmt maximal den Wert eins an. Der Wert des korrigierten r^2 liegt im vorliegenden Modell bei 0,41. Fast alle einbezogenen Variablen haben einen signifikanten Effekt auf die Sorge in Bezug auf Datensicherheit beim Onlineshopping und erklären diese somit gut.

Im Anhang werden die Variablen aufgelistet, die in das Modell eingegangen sind (Tabelle 90).

Da einige Variablen inhaltlich zwar einen Effekt auf den Grad der Besorgtheit vermuten ließen, statistisch aber miteinander korrelierten (Korrelationen von >= 0,4), wurden diese Variablen nicht in das Modell aufgenommen. Die ausgeschlossenen Variablen sind in Tabelle 91 enthalten.

Es zeigt sich, dass...

- das Ausmaß an Bedenken, die beim Onlineshopping vorhanden sein können (z. B. Ware kommt nicht bzw. falsch oder beschädigt an, es handelt sich nicht um einen tatsächlichen Onlineshop, etc.), einen signifikant positiven Effekt auf den Grad der Besorgtheit im Hinblick auf die Datensicherheit beim Onlineshopping haben: Je höher die einzelnen Bedenken ausgeprägt sind, desto größer auch der Grad der Besorgtheit hinsichtlich der Datensicherheit beim Onlineshopping.
- das Ausmaß des Interesses für das Thema keinen signifikanten Effekt auf den Grad der Besorgtheit hat. Wie oben beschrieben wurde, gibt es zwar einen bivariaten Zusammenhang zwischen Befragten mit hohem (Top-2-Box) bzw. niedrigem Grad der Besorgtheit (Low-2-Box) und dem Interesse am Thema (betrachtet auf Top-2-Box-Basis). Dieser kann allerdings auf höherer Ebene der Regression nicht identifiziert werden, so dass eine je höher desto Aussage nicht abgeleitet werden kann – auch wenn in einzelnen Punkten das thematische Interesse einen Einfluss auf die Wahrnehmung und den Umgang mit Datensicherheitsaspekten beim Onlineshopping hat.
- die Einschätzung der Wahrscheinlichkeit eines Schadensfalls einen signifikant positiven Effekt auf den Grad der Besorgtheit hat: Je höher die Wahrscheinlichkeit eingeschätzt wird, dass die persönlichen Daten beim Onlineshopping von Dritten unrechtmäßig eingesehen oder entwendet werden, desto höher der Grad der Besorgtheit. Wenn Befragte einschätzen, dass sie betroffen sein könnten, sind sie auch besorgter.
- die Einschätzung des Grads der Gefährlichkeit verschiedener Aspekte, die beim Onlineshopping passieren können (wie z. B. Bank- bzw. Kreditkartendaten werden entwendet), einen signifikant positiven Effekt auf den Grad der Besorgtheit haben. Je bewusster sich Befragte über die möglichen Gefahren sind, desto besorgter sind sie im Hinblick auf die Datensicherheit beim Onlineshopping.
- das Informiertheitsgefühl (bzw. Schutzgefühl) durch staatliche Institutionen keinen signifikanten Effekt auf den Grad der Besorgtheit im Hinblick auf die Datensicherheit beim Onlineshopping hat – es kann also keine je höher desto Aussage getroffen werden.
- ein bereits erfolgtes Informieren in der Vergangenheit zum Thema auch zu einem höheren Besorgnisniveau führt. Ähnlich zur Einschätzung der Schadenswahrscheinlichkeit kann davon ausgegangen werden, dass je relevanter das Thema für die Befragten persönlich ist, desto größer ist auch deren Besorgnis.
- persönliche negative Erfahrungen mit dem Thema einen signifikant positiven Effekt auf die Besorgnis haben. Dieses Ergebnis geht mit der eben beschriebenen persönlichen Relevanz des Themas für die Befragten einher.
- die Vorsichtigkeit in Bezug auf persönliche Daten generell einen positiven Effekt auf den Grad der Besorgtheit haben – je vorsichtiger jemand ist, desto größer auch die Besorgnis.

- die Selbstwirksamkeit einen signifikant negativen Effekt auf Besorgtheit hat: Je eher sich Befragte selbst in der Lage fühlen, einen Beitrag zur Erhöhung der Datensicherheit beim Onlineshopping zu leisten, desto niedriger der Grad der Besorgtheit.

4.3.3 Datensicherheit: Verständnis, Informiertheit, Gefahreneinschätzung

Wie ist es um das Risikobewusstsein und die Beurteilungsfähigkeit von Verbraucherinnen und Verbrauchern mit Blick auf Datenleak-Vorfälle bestellt? Mit Blick auf das Risikobewusstsein bedeutet dies, inwiefern sich Verbraucherinnen und Verbraucher sich der potenziell negativen Auswirkungen eines Verlusts ihrer persönlichen Daten bewusst sind.

Um diesen Fragen nachzugehen, erfolgte eine Betrachtung des Verständnisses, der Informiertheit und der Gefahreneinschätzung der Befragten zum Thema Datensicherheit. Welches Verständnis von Datensicherheit liegt zugrunde? Haben sich die Befragten schon einmal zum Thema informiert und wo haben sie sich informiert? Welche Relevanz hat die Datensicherheit beim Onlineshopping für die Verbraucherinnen und Verbrauchern und welche möglichen Gefahren im Zusammenhang mit Datensicherheit beim Onlineshopping sehen die Befragten und welche wird dabei als am größten eingeschätzt?

4.3.3.1 Definition Datensicherheit

Die meisten Befragten (83 Prozent) waren auf Basis einer gestützten Abfrage, bei der sie aus vorgegebenen Antwortmöglichkeiten, die für sie zutreffendste auswählen konnten, der Meinung, Datensicherheit bedeute, dass Zahlungsdaten sicher verschlüsselt werden und sie auf diese Weise vor finanziellem Schaden geschützt seien, sofern diese hinterlegt werden müssten. Ebenfalls 83 Prozent der Befragten gaben an, dass ihrer Meinung nach Datensicherheit beim Onlineshopping bedeutet, dass das Passwort für den Login zum Kundenbereich sicher verschlüsselt wird. Nahezu drei Viertel aller Befragten verstehen unter Datensicherheit, persönliche Daten werden nicht unrechtmäßig von Dritten eingesehen oder entwendet. Mit etwa 69 Prozent sind etwas weniger Befragte der Ansicht, dass Datensicherheit beim Onlineshopping bedeutet, persönliche Daten werden nicht an Dritte weitergegeben. Und für etwas mehr als die Hälfte bedeutet Datensicherheit beim Onlineshopping, dass die Liste der Einkäufe nicht an Dritte weitergegeben wird. Auch, dass Informationen über Einkäufe nicht für Werbung genutzt werden, stellt für vier von zehn Befragten einen Aspekt der Datensicherheit dar. Diese Aufzählung macht deutlich, welch heterogenes Bild die Verbraucherinnen und Verbraucher haben, wenn es um die Datensicherheit beim Einkauf im Internet geht.

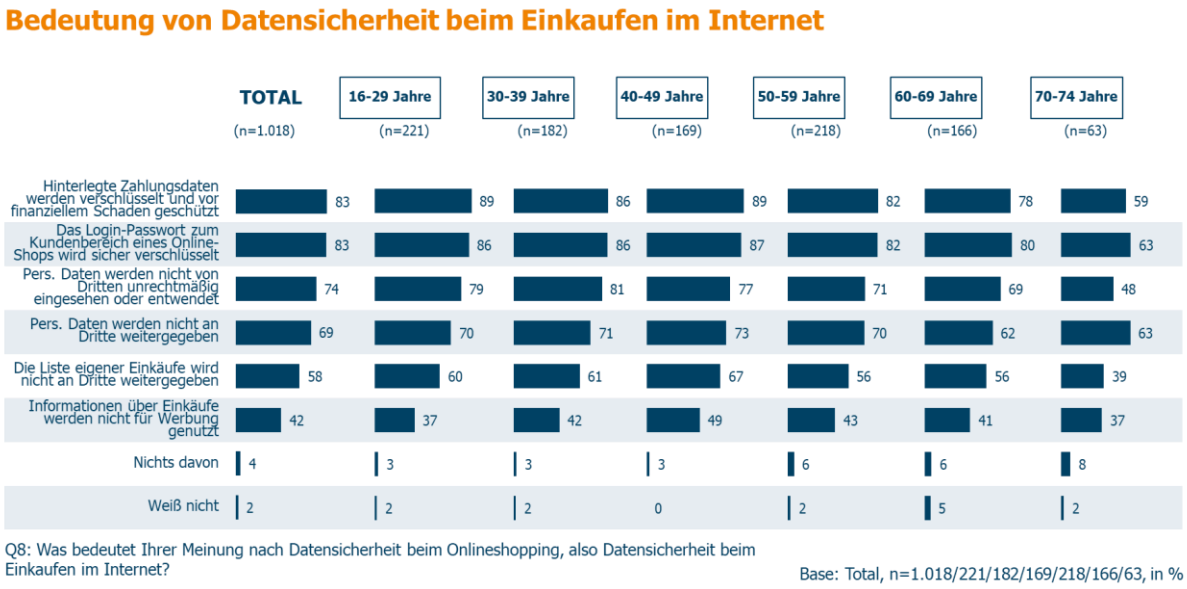


Abbildung 9 Bedeutung von Datensicherheit beim Einkaufen im Internet nach Alter

Für Befragte, die häufig Onlineeinkäufe tätigen, ist die sichere Verschlüsselung des Passworts im Kundenbereich mit 91 Prozent die am häufigsten ausgewählte Definition. Weiter lässt sich feststellen, dass die Definition, die im Einklang mit der des BSI steht, nämlich „meine persönlichen Daten werden nicht von Dritten unrechtmäßig eingesehen oder entwendet“, zwar mit 74 Prozent eine hohe Antwortrate aufweist, andererseits eine Vielzahl Definitionen, die andere Aspekte fokussieren, ebenfalls hohe Zustimmungswerte erhalten haben. Auch hieran wird deutlich, dass bei Verbraucherinnen und Verbrauchern ein unscharfes, breites Verständnis von Datensicherheit beim Onlineshopping vorherrschend ist. Der Schutz der Zahlungsdaten und damit der Schutz vor finanziellen Risiken steht im Vordergrund (83 Prozent). Dies brachte auch ein Verbraucher in den qualitativen Interviews zum Ausdruck:

> *„Bei einem Shop, den ich nicht kenne und bei dem ich zum ersten Mal eine Bestellung aufgebe, gebe ich keine Kreditkartendaten ein! Am Ende sitzt man auf einem finanziellen Schaden auf!“*

Für die Kommunikation sollte dieses vielschichtige Verständnis berücksichtigt und die zu kommunizierende Botschaft geschärft werden, um Missverständnisse zu vermeiden. Das Wort Datensicherheit allein hat für Verbraucherinnen und Verbraucher keineswegs einen eindeutigen und klar umrissenen Inhalt.

4.3.3.2 Informiertheit

Rund die Hälfte der Befragten gab an, sie hätten sich schon einmal zum Thema Datensicherheit beim Onlineshopping informiert.

Deutliche Unterschiede hinsichtlich Alter oder Geschlecht sind nicht zu erkennen, jedoch auf den Variablen Schulbildung, Onlineshopping-Erfahrung und dem Interesse an Datensicherheit:

- Mit 57 Prozent sind es besonders Befragte mit hoher formaler Schulbildung im Vergleich zu Befragten mit niedrigerer formaler Schulbildung (Volks- bzw. Hauptschule 43 Prozent), die sich schon einmal zum Thema Datensicherheit beim Onlineshopping informiert haben.
- Besonders diejenigen, die häufig im Internet einkaufen (mindestens ein- oder mehrmals pro Woche), gaben an, sich schon einmal zum Thema Datensicherheit beim Onlineshopping informiert zu haben (67 Prozent).
- Fast zwei Drittel derjenigen, die sich sehr für das Thema Datensicherheit interessieren, haben sich auch schon einmal aktiv zum Thema informiert.

Wenn sich die Verbraucherinnen und Verbraucher schon einmal zum Thema Datensicherheit beim Onlineshopping informiert haben, nutzten Sie dafür im Schnitt drei unterschiedliche Quellen. Die Anzahl der konsultierten Informationsquellen nimmt dabei mit zunehmendem Lebensalter ab: Gaben 16-29-Jährige im Schnitt fünf Quellen an, so sind es bei den 40-49-Jährigen rund drei unterschiedliche Quellen, ebenso bei den 60-69-Jährigen. 70-74-Jährigen verwenden rund zwei Quellen:

- Die am häufigsten genannte Informationsquelle ist mit Abstand das Internet allgemein (z. B. über Suchmaschinen): 78 Prozent gaben an, sich hier zum Thema Datensicherheit beim Onlineshopping informiert zu haben.
- Mit deutlichem Abstand nach dem Internet folgen Freunde, Familie, Kollegen als zweitwichtigste Informationsquelle, die knapp jede(r) zweite Befragte heranzieht, um sich zum Thema Datensicherheit beim Onlineshopping zu informieren.
- Über Fernsehen bzw. Mediatheken informieren sich 36 Prozent der Befragten.
- 32 Prozent informieren sich in Tages- oder Wochenzeitungen.
- Weniger häufig genutzte Informationsquellen sind die Verbraucherzentrale bzw. Verbraucherschutz (29 Prozent), spezielle Foren bzw. Blogs bzw. Podcasts (27 Prozent), Behörden allgemein (23 Prozent),

Video- bzw. Streaming Plattformen, z. B. YouTube (23 Prozent), das BSI (21 Prozent), soziale Medien (19 Prozent) oder das Radio (18 Prozent).

Bei der Nutzung des Internets allgemein als Informationsquelle zeigt sich ein Einfluss des Alters und der Häufigkeit des Onlineshoppings:

- Vor allem Befragte zwischen 16 und unter 60 Jahre informieren sich über das Internet. Einen Schwerpunkt bilden die 40-49-Jährigen.
- Es zeigt sich auch eine Korrelation mit der Häufigkeit des Onlineshoppings. Über 80 Prozent der Befragten, die häufiger online shoppen, gaben an, sich im Internet allgemein zum Thema Datensicherheit beim Onlineshopping zu informieren.

Besonders für die jüngste Altersgruppe (16-29-Jährige) ist das soziale Umfeld als Informationsquelle wichtig. Sie informieren sich deutlich häufiger bei Freunden, Familie und Kollegen als ältere Altersgruppen (57 Prozent 16-29-Jährige vs. 30 Prozent 70-74-Jährige).

Ob Befragte Fernsehen und Mediatheken (36 Prozent) als Informationsquelle heranziehen oder Tages- oder Wochenzeitung (32 Prozent) unterscheidet sich vor allem in Bezug auf das Alter. Die Nutzung nimmt hier mit dem Lebensalter deutlich zu. Aber auch das Interesse am Thema zeigt eine deutliche Korrelation: Gut ein Drittel der Personen, die ein hohes Interesse an dem Thema haben, informieren sich über Tages- oder Wochenzeitungen. In der Vergleichsgruppe, der nicht am Thema Datensicherheit Interessierten, sind es 24 Prozent.

Auch mit Blick darauf, wer eine Verbraucherzentrale bzw. den Verbraucherschutz als Informationsquelle nutzt, zeigen sich vor allem Unterschiede entlang des thematischen Interesses: Knapp ein Drittel der Interessierten informiert sich hier – bei den Nicht-Interessierten sind es 24 Prozent.

Spezielle Blogs bzw. Foren und Podcasts im Internet als Informationsquelle sowie Video- und Streaming-Plattformen nutzen besonders häufig Jüngere bis 49 Jahre, dabei vornehmlich die 16-29-Jährigen (41Prozent Video- bzw. Streaming-Plattformen, 39 Prozent Blogs bzw. Foren). Des Weiteren werden diese Informationsquellen ebenso öfter genutzt, wenn die Befragten häufig Onlineshopping betreiben oder bereits negative Erfahrung mit Datensicherheit gemacht haben (35 Prozent in Blogs bzw. Foren, 33 Prozent Video-bzw. Streaming-Plattformen).

Behörden allgemein werden, genauso wie das BSI, öfter von Männern (30 Prozent Behörden, 26 Prozent BSI) als von Frauen (Behörden 16 Prozent, BSI 16 Prozent) als Informationsquelle genannt, um sich zum Thema Datensicherheit beim Onlineshopping zu informieren.

Über soziale Medien informieren sich vor allem jüngere Befragte (38 Prozent) wohingegen Befragte ab 60 Jahren dies nur sehr selten mit einstelligem Prozentsatz tun (60-69-Jährige: 6 Prozent; 70-74-Jährige: 1 Prozent). So sind es aber auch generell die Jüngeren, die soziale Medien nutzen. Zusätzlich lässt sich eine vermehrte Nutzung von sozialen Medien als Informationsquelle dann feststellen, wenn die Befragten häufig online einkaufen (35 Prozent vs. 18 Prozent selten) oder kein großes Interesse an dem Thema Datensicherheit mitbringen (36 Prozent vs. 15 Prozent der am Thema Interessierten).

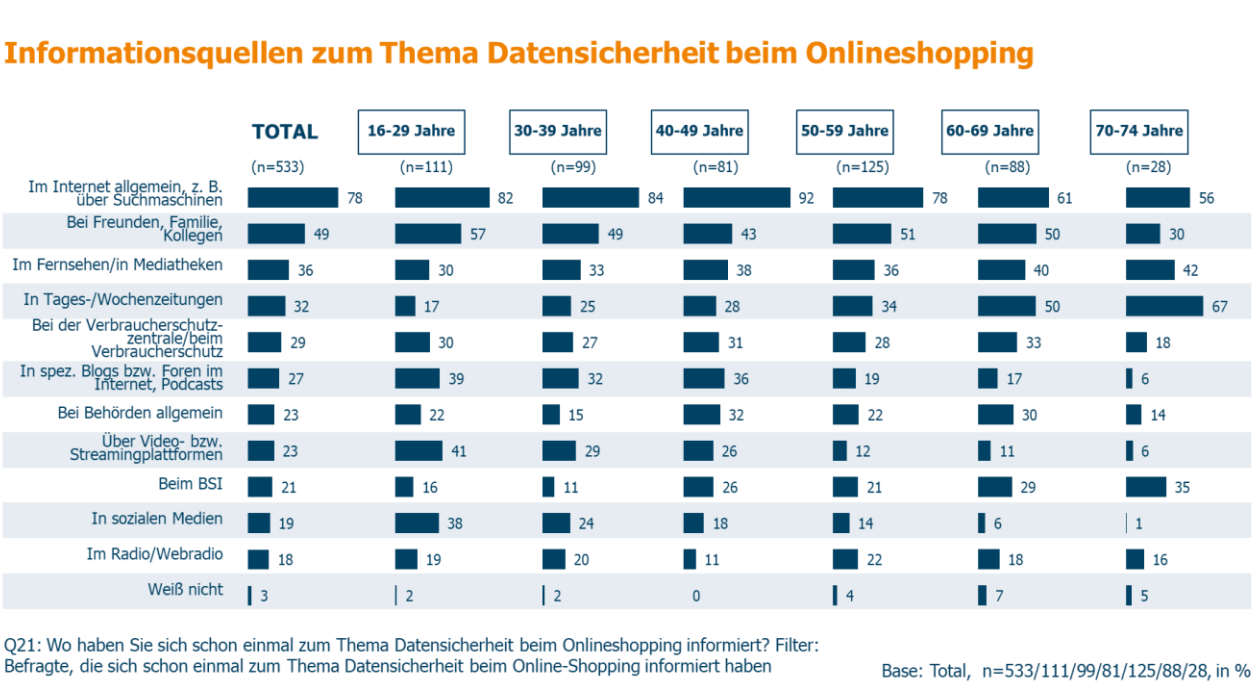


Abbildung 10 Informationsquellen zum Thema Datensicherheit beim Onlineshopping nach Alter

Zusammenfassend lässt sich festhalten, dass es insbesondere Befragte mit hoher formaler Schulbildung sind, die angaben sich zum Thema Datensicherheit zu informieren. Darüber hinaus spielt das Einkaufsverhalten eine Rolle. Denn Verbraucherinnen und Verbraucher, die online einkaufen und dies zudem häufig tun, informieren sich häufiger zum Thema als alle anderen Befragten. Das Interesse am Thema ist entscheidend, wenn es darum geht, aktiv Informationen einzuholen und hat auch Einfluss auf die genutzten Informationsquellen. Befragte, die sich informieren, nutzen überwiegend das Internet (z. B. über Suchmaschinen) und suchen Rat bei Freunden, Familienmitgliedern oder Kollegen. Vor allem wenn sie jünger sind. Seltener informieren sich Verbraucherinnen und Verbraucher bei Behörden oder dem BSI.

4.3.3.3 Gefahreneinschätzung

Im Folgenden wird beleuchtet, wie es um die Gefahreneinschätzung der Verbraucherinnen und Verbraucher bestellt ist. Welche möglichen Gefahren im Zusammenhang mit Datensicherheit beim Onlineshopping sehen die Befragten und welche wird dabei als am größten eingeschätzt?

In der qualitativen Untersuchung ergaben sich bereits Hinweise darauf, dass Verbraucherinnen und Verbraucher nicht genau wissen, worin eigentlich der Schaden bei einem Datenleak-Vorfall für sie liegen könnte. Zur Einschätzung der Gefahren zum Thema Datensicherheit im Onlineshopping wurden diese in der Quantifizierung gestützt und in Relation zu anderen Gefahren im Internet abgefragt. Daraus ergibt sich ein geeignetes Bild, was Motivatoren sein könnten, sich mit dem Thema Datensicherheit vermehrt auseinander zu setzen, nämlich der Diebstahl von Bank- bzw. Kreditkartendaten oder ein potenzieller Identitätsdiebstahl.

Ein Großteil der Befragten fürchtet vor allem folgende Gefahren beim Onlineshopping:

- Diebstahl von Bank- bzw. Kreditkartendaten (Top-2-Box: 63 Prozent).
  Besonders ausgeprägt ist dies bei 16-29-Jährigen (Top-2-Box: 73 Prozent) bzw. bei Frauen (Top-2-Box: 67 Prozent vs. 58 Prozent Männer), sowie bei Befragten mit höherer Bildung (Top-2-Box: 72 Prozent derjenigen mit Abitur vs. 49 Prozent formal niedrige Bildung) und bei denjenigen, die seltener online einkaufen (Top-2-Box: 70 Prozent);
- Weiterreichen von persönlichen Daten wie Name, Adresse etc. (Top-2-Box: 58 Prozent).
  Hier sind es vor allem die 60-69-Jährigen (Top-2-Box: 67 Prozent) und diejenigen, die nur moderat oder

selten im Internet einkaufen (Top-2-Box: mindestens sechs von zehn der Befragten vs. nur vier von zehn bei denjenigen, die häufig online einkaufen);

- Missbrauch der persönlichen Daten für Identitätsdiebstahl (Top-2-Box: 58 Prozent).

Des Weiteren gilt den Befragten zufolge als gefährlich:

- Hacking des Passworts zum E-Mailzugang (Top-2-Box: 57 Prozent). Dies betrifft vor allem jüngere Befragte zwischen 16 und 39 Jahren.
- Infizieren eines Gerätes mit Schadsoftware (Top-2-Box: 56 Prozent), z. B. mit Viren oder Trojanern, so dass dieses nicht mehr nutzbar ist.
- Verschlüsselung persönlicher Daten auf einem Gerät, so dass dieses nicht mehr genutzt werden kann (Top-2-Box: 42 Prozent).
- Das Weiterreichen der Einkaufsliste stellt für rund ein Viertel der Befragten eine Gefahr im Zusammenhang mit Onlineshopping dar, vor allem für ältere Befragte ab 40 Jahren (Top-2-Box: mind. 30 Prozent).

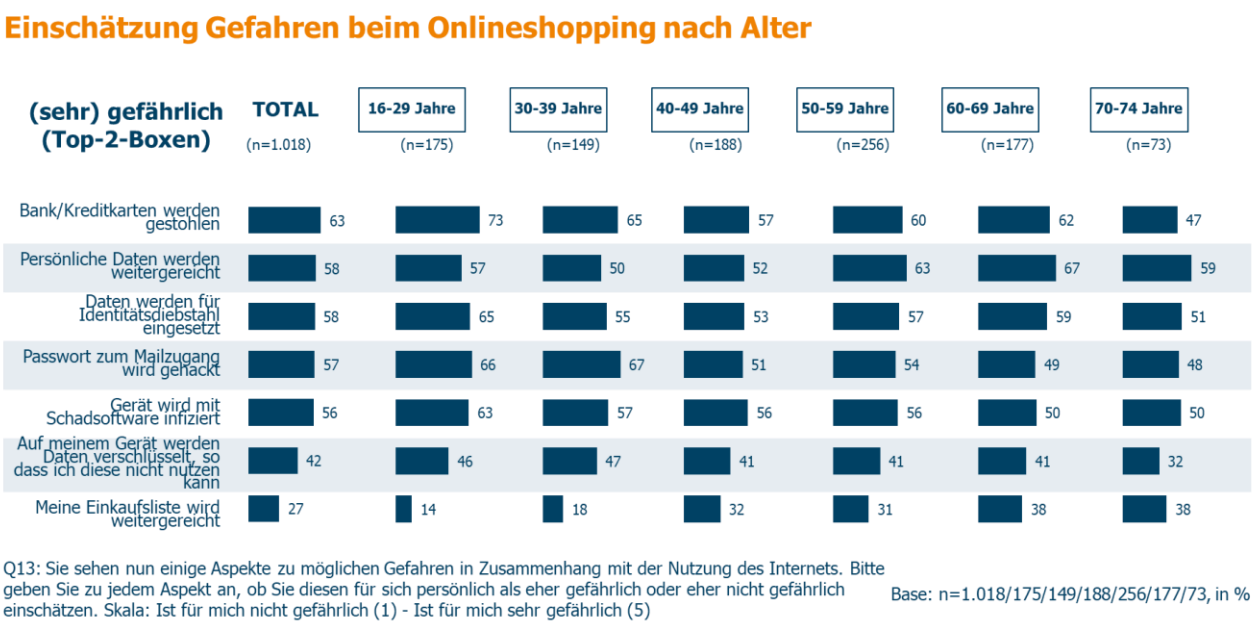


Abbildung 11 Einschätzung Gefahren beim Onlineshopping nach Alter

Einerseits führt die Nennung möglicher Gefahren im Internet zu relativ hohen Zustimmungswerten. Andererseits zeigt der hohe Anteil derjenigen, die zumindest gelegentlich (91 Prozent) bzw. häufig im Internet einkaufen (55 Prozent), dass Onlineshopping für Verbraucherinnen und Verbraucher viele Vorteile bietet, die für sie weit eher im Vordergrund stehen und das Onlineshopping trotz Gefahren attraktiv erscheinen lassen. Dieses Ergebnis spiegelt sich auch in den Ergebnissen der qualitativen Befragung wider. Das Thema Datensicherheit rückt beim Onlineshopping häufig stark in den Hintergrund. Darauf weist auch die angenommene Eintrittswahrscheinlichkeit eines persönlichen Schadensfalls hin – rund 25 Prozent (Low-2-Box) schließen diesen für sich aus, 38 Prozent sind unsicher bis unentschieden und nur gut ein Drittel hält diesen für wahrscheinlich (Top-2-Box). Oft, so legen die qualitativen Interviews nahe, geht es Verbraucherinnen und Verbrauchern beispielsweise deutlich mehr um Bequemlichkeit bzw. Komfort, die Einfachheit des Einkaufs, den Eindruck günstige Preise erwirken zu können oder die schnelle Verfügbarkeit von Waren. Erst wenn es um den Diebstahl von Zahlungsdaten oder dem unrechtmäßigen Entwenden und Zweckentfremden persönlicher Daten geht, entsteht Aufmerksamkeit auf das Thema Datensicherheit beim Onlineshopping.

4.3.4 Betroffenheit und Verhalten im Schadensfall

Rund ein Viertel der Befragten gab an, bereits einmal negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht zu haben, also dass persönliche Daten von Dritten unrechtmäßig eingesehen oder entwendet wurden. Die Befragten sollten außerdem angeben, was sie in dieser Situation getan haben bzw. tun würden, wenn sie negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht haben bzw. machen würden.

- Die am häufigsten genannte Reaktion (neun von zehn Befragte) war Passwörter zu ändern. Vor allem Personen zwischen 30-39 Jahren (94 Prozent) gaben die Passwortänderung als Reaktion an.
- Als am zweithäufigsten genannte Maßnahme haben bzw. würden die Befragten Kontakt mit den Shop-Betreibenden aufnehmen (73 Prozent).
- Zwei Drittel der Befragten gaben an, dass sie Accounts, bei denen sie persönliche Daten hinterlegt hatten, zurückgesetzt bzw. gelöscht haben bzw. dies im Falle negativer Erfahrung tun würden. Dies nannten insbesondere Befragte im Alter zwischen 30-69 Jahre im Vergleich zur jüngsten oder ältesten Altersgruppe.
- Insgesamt 64 Prozent würden Kontakt mit der Polizei aufnehmen bzw. haben dies getan, vor allem ältere Befragte zwischen 60-74 Jahren vergleichsweise häufig (75 Prozent 60-69-Jährige, 87 Prozent 70-74-Jährige).
- Die Hälfte der Befragten holt sich Rat bei Freunden bzw. Bekannten bzw. der Familie. Hier sind es insbesondere die 16-29-Jährigen (67 Prozent) und außerdem Befragte, die generell nicht am Thema Datensicherheit interessiert sind (64 Prozent Nicht-Interessierte vs. 43 Prozent Sehr Interessierte), die im persönlichen Umfeld um Rat fragen.

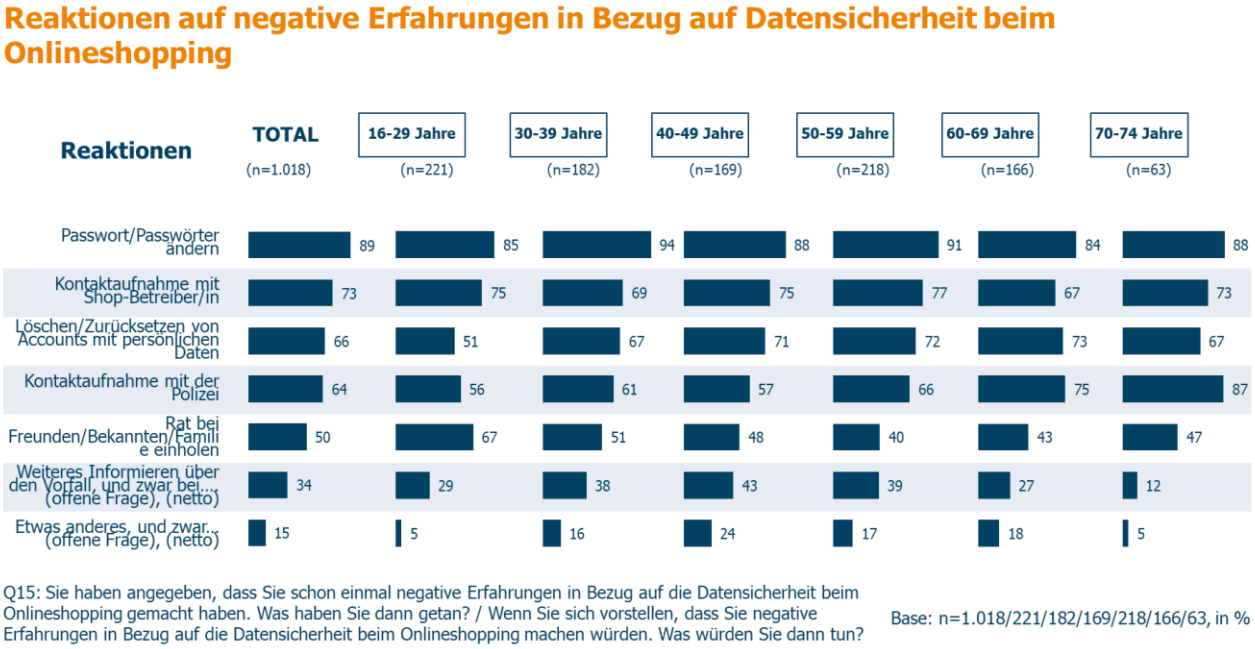


Abbildung 12 Reaktionen auf negative Erfahrungen beim Onlineshopping nach Alter

Weitere Reaktionen auf negative Erfahrung in Bezug auf die Datensicherheit beim Onlineshopping:

- Drei von zehn Befragte würden sich weiter zu dem Vorfall informieren. Zurückgreifen würde sie dabei vor allem auf:
  - Suchmaschinen im Internet (21 Prozent)
  - die Verbraucherzentrale (fünf Prozent)
  - Foren (zwei Prozent)

- Banken bzw. Kreditunternehmen (ein Prozent)
- Rechtsschutz (ein Prozent)
- Behörden allgemein (ein Prozent)
- BSI (ein Prozent)
- IT-Spezialisten (ein Prozent).

Insgesamt 34 Prozent der Befragten würden sich weiter zu dem Vorfall informieren, und zwar mit deutlichem Abstand am häufigsten im Internet bzw. über Suchmaschinen (21 Prozent der Befragten). Hier sind es im Vergleich zu den 70-74-Jährigen besonders die Jüngeren, die sich weiter im Internet bzw. über Suchmaschinen zu dem Vorfall informiert haben bzw. informieren würden (drei Prozent der 70-74-Jährigen vs. 24 Prozent der 16-29-Jährigen bzw. 22 Prozent der 30-39-Jährigen bzw. 28 Prozent der 40-49-Jährigen).

- Insgesamt vier Prozent würden als Reaktion auf eine entsprechende Erfahrung generell weniger Onlineshopping betreiben.
- Drei Prozent haben bzw. würden das Bankinstitut informieren,
- Zwei Prozent haben bzw. würden personenbezogene Daten löschen.
- Jeweils ein Prozent der Befragten hat bzw. würde eine Sicherheitssoftware installieren oder hat bzw. würde andere entsprechend warnen.
- Lediglich zwei Prozent würden gar nichts tun bzw. haben gar nichts getan oder wissen es nicht, was sie tun würden bzw. getan haben.

Neben den Reaktionen auf einen (möglichen) Datenleak-Vorfall wurden die Befragten außerdem noch gebeten, ihre Meinung zu verschiedenen Einstellungsfragen im Zusammenhang mit der Datensicherheit im Internet zu äußern. Dabei ist die große Mehrheit insgesamt davon überzeugt, dass es gesetzliche Vorgaben gibt, um die Sicherheit beim Onlineshopping zu gewährleisten. 85 Prozent bejahten die Aussage, dass Onlineshops gesetzlich dazu verpflichtet sind, die Sicherheit der persönlichen Daten zu gewährleisten. Auch wenn die Mehrheit der Verbraucherinnen und Verbraucher etwas unternommen hat bzw. unternehmen würde, wenn es zu einem Vorfall in Bezug auf die Datensicherheit kam bzw. käme, kann die These zwar widerlegt werden, dass Verbraucherinnen und Verbraucher resignieren und nichts unternehmen. Dennoch ist der Wunsch nach Orientierung in diesem Kontext sehr deutlich ausgeprägt. Als Orientierungshilfe bei der Einschätzung der Sicherheit von Anbieterinnen und Anbietern können nach Ansicht der Verbraucherinnen und Verbraucher zum einen die Größe eines Onlineshops bzw. einer Plattform sowie Siegel von einer unabhängigen dritten Stelle bzw. staatlicher Seite dienen:

- So kann die These bestätigt werden, dass je größer die Onlineshopping-Plattform ist, desto mehr Vertrauen haben die Verbraucherinnen und Verbraucher: 60 Prozent der Personen, die zumindest gelegentlich im Internet einkaufen, stimmten der Aussage zu, dass sie beim Onlineshopping eher großen als kleinen Onlineshops oder Plattformen im Hinblick auf die Datensicherheit vertrauen.
- Auch die These, dass Verbraucherinnen und Verbraucher ein Siegel von einer unabhängigen dritten Stelle bzw. von staatlicher Seite zur Kennzeichnung sicherer Onlineshops wünschen, ist zutreffend. So wünscht sich die Mehrheit der Befragten eine Orientierungshilfe, um die Sicherheit von Anbieterinnen und Anbietern besser einschätzen zu können: Acht von zehn Befragten wünschen sich ein Siegel von einer unabhängigen dritten Stelle, welches die Sicherheit von Onlineshops bewertet und Orientierung bei der Auswahl eines Onlineshops bietet. Daneben wünschen sich 68 Prozent ein Siegel von staatlicher Seite, welches die Sicherheit von Onlineshops bewertet und Orientierung bei der Auswahl eines Onlineshops bietet.

Die Befragung hat verdeutlicht, dass sich Verbraucherinnen und Verbraucher von staatlicher Seite mehr Information zum und Orientierung beim Thema Datensicherheit im Onlineshopping wünschen. Ähnlich äußerten sich auch die Expertinnen und Experten aus der qualitativen Untersuchung, wonach Verbraucherinnen und Verbraucher deutlich auf die Auswirkungen von Datenleak-Vorfällen hingewiesen

werden müssten. Die in diesem Zusammenhang geführten Gespräche mit Verbraucherinnen und Verbrauchern legen nahe, dass Szenarien, die den potenziellen Identitätsdiebstahl als Schadens-Szenario, aber auch Zahlungsverkehrsdaten thematisieren (Daten von Bank- und Kreditkarten), die abhandenkommen können, eine entsprechende Überzeugungskraft entwickeln können.

- Rund die Hälfte der Befragten, die zumindest gelegentlich online einkaufen, wüsste nicht genau, welche Auswirkungen das Entwenden bzw. unrechtmäßige Einsehen ihrer Daten für sie persönlich hätte.
- 81 Prozent der Befragten, die zumindest gelegentlich in Onlineshops einkaufen, nehmen an, dass das unrechtmäßige Einsehen oder Entwenden der eigenen Daten sehr wahrscheinlich negative Auswirkungen auf sie selbst hätte.
- Nur rund die Hälfte der Befragten, die zumindest gelegentlich in Onlineshops einkaufen, wüsste, wohin sie sich wenden können, wenn bei einem Onlineshop, bei dem sie Kunde sind, Daten entwendet wurden.

Die Antworten zeigen, dass Verbaucherinnen und Verbrauchern den konkreten persönlichen Schaden bei einem Datenleak-Vorfall oft nicht realisieren und ihnen damit die Auswirkungen nicht bewusst sind. Dies mag vor allem an einem fehlenden, unmittelbaren Schadenserlebnis liegen.

Zusammenfassend lässt sich hinsichtlich der Betroffenheit und des Verhaltens im Schadenfall der Befragten festhalten, dass ungefähr ein Viertel schon einmal negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht hat. Das Passwort zu ändern, war die am häufigsten genannte Reaktion auf einen Datenleak-Vorfall. Aber auch den Shop-Betreiber bzw. die Shop-Betreiberin zu kontaktieren oder die Accounts, bei denen persönliche Daten hinterlegt wurden, zurückzusetzen bzw. zu löschen sowie Kontakt mit der Polizei aufzunehmen oder Freunde, Bekannte bzw. die Familie um Rat zu fragen, zählen zu den am häufigsten genannten Maßnahmen.

4.3.5 Schutzmaßnahmen

Wie bereits deutlich wurde, zeigt sich eine Mehrheit der Befragten generell mit einem Bewusstsein dafür, dass Onlineshopping gewisse Gefahren im Hinblick auf die Datensicherheit birgt. Inwieweit Verbraucherinnen und Verbraucher versuchen, diesen Gefahren durch gezielte Maßnahmen entgegenzuwirken, ist Gegenstand des folgenden Kapitels.

Die Expertinnen und Experten aus der qualitativen Befragung sind der Auffassung, dass die Handlungsmöglichkeiten von Verbraucherinnen und Verbrauchern zum Schutz ihrer persönlichen Daten im Onlineshopping limitiert sind. Andreas Sachs vom Bayerischen Landesamt für Datenschutzaufsicht ist der Ansicht:

> *„Wenn es einen Sicherheitsvorfall gibt, also meine Daten sind vielleicht weg, vielleicht auch mein Passwort, da hat man als Verbraucherin oder Verbraucher ja gar keine Kontrolle darüber, ob der Shop die Daten überhaupt ordentlich verschlüsselt oder transformiert gespeichert hat oder nicht.“*
> (Andreas Sachs, Bayerisches Landesamt für Datenschutzaufsicht)

Hinzu kommt erschwerend, dass direkt beim Einkauf Verbraucherinnen und Verbraucher keine unmittelbaren Schadenerfahrungen machen können. Es entsteht kein unmittelbares Schadenerlebnis, das zu einer Erhöhung des Besorgnislevels, der Motivation sich zu informieren oder zu einer erhöhten Bereitschaft führen könnte, sich über Gegenmaßnahmen zu informieren.

So konstatiert auch Stefanie Siegert von der Verbraucherzentrale Sachsen den Anspruch, dass Datensicherheit für die Verbraucherinnen und Verbraucher so einfach wie möglich gehalten werden muss. Denn deren primäres Ziel ist der Einkauf, nicht die Überprüfung von Datensicherheit:

> *„Was ist das Ziel des Verbrauchers? Der möchte einfach die Ware in diesem Onlineshop bestellen. Und jetzt zu erkennen, welche Systematik dieser Shop hat? Ob das irgendeine Art von Shop-in-Shop, ob das irgendein Verkäufer von Ebay ist, der sich auch bei Amazon*

> *herumtreibt und so weiter? Dass er da vielleicht noch Untersuchungen anstellt? Das werden die Verbraucher nicht tun. Insofern ist der Anspruch, es muss für Verbraucher so einfach wie möglich sein. Also in dem Moment, in dem Ware veräußert wird von einem Unternehmen an Verbraucherinnen und Verbraucher, muss dieser Webshop einfach sicher sein."*
> (Stefanie Siegert, Verbraucherzentrale Sachsen)

Im Hinblick auf das Erstellen und den Umgang mit Passwörtern sehen Expertinnen und Experten die Verbraucherinnen und Verbraucher in der Pflicht:

> *„Man hat [als Verbraucherin und Verbraucher] die Kontrolle darüber, ob dieses Passwort für einen anderen Onlinedienst, für einen anderen Shop zweckentfremdet wird oder nicht, indem man ein Passwort nie auch bei anderen Shops oder Onlinediensten verwendet, ... und starke, d. h. komplexe und bzw. oder lange Passwörter wählt, die schlecht erraten werden können. Aus Verbrauchersicht kann man nicht mehr machen, es ist ja auch Aufgabe der Onlineshops, eine ausreichende Sicherheit zu gewährleisten."*
> (Andreas Sachs, Bayerisches Landesamt für Datenschutzaufsicht)

Für die Zukunft erhofft sich Herr Sachs:

> *„..., dass gesetzliche Regulatorien zur Sicherstellung eines Schutzniveaus greifen, und dass vielleicht die Sicherheitscommunity umtriebig ist, manche Lücken findet und diese den entsprechenden Stellen wie die Datenschutzaufsichtsbehörden dann auch meldet, damit diese Stellen auch an die Betreiber im Zweifel herantreten und Sicherheitsmängel kraft ihrer gesetzlichen Aufgaben abstellen."*
> (Andreas Sachs, Bayerisches Landesamt für Datenschutzaufsicht)

Einen Schritt weiter geht Jan Mahn vom Heise-Verlag, indem er eher die Seite der (professionellen) Shop-Ersteller (Webagenturen) in der Pflicht sieht, sich selbst zuverlässig fortzubilden, um die Gefahr von Datenleaks zu reduzieren:

> *„Ich glaube, wir sind ganz kurz davor, dass wir eine Meisterpflicht für IT-Berufe bräuchten. Sicher wäre das ein riesiges Problem, wenn wir sie einführen würden. Wir haben in Deutschland mit Recht verschiedene Meisterpflichten. Aber im IT-Bereich darf jeder eine Webshop-Agentur aufmachen, wenn man schon mal einen Webshop für jemanden gebaut hat! Ich glaube, dass gerade Handwerksmeister z. B. im Elektro-Bereich eine qualifizierte Ausbildung bekommen. In der IT haben wir so ein Verständnis leider nicht. Im Studium wird das nicht vermittelt, da wird bei IT-Security über teils sehr hochtrabende Dinge geredet, auf die offensichtlichen Schutzmaßnahmen gegen die Feld-Wald-und-Wiesen-Angriffe wird aber zu wenig eingegangen."*

Im Rahmen der Verbraucherbefragung wurde nun untersucht, welche Maßnahmen die Befragten zum Schutz ihrer persönlichen Daten im Internet allgemein wie auch konkret beim Onlineshopping anwenden.

Die Mehrheit der Befragten gab an, dass sie allgemein konkrete Schutz- bzw. Vorsichtsmaßnahmen anwenden. Diese sind:

- 80 Prozent der Befragten lehnen die Nutzung personenbezogener Daten für Werbezwecke ab.
- 68 Prozent der Befragten speichern Daten (z. B. Kopien von Führerschein, Personalausweis, Gesundheitskarte) nicht in einem Online-Speicher (Cloud).
- 68 Prozent der Befragten beschränken den Zugriff auf geografische Standortdaten
- 64 Prozent der Befragten teilen bei der Nutzung sozialer Medien ihre Profilinhalte nur mit Personen, die Mitglieder ihres sozialen Netzwerks sind.

Folgende Schutzmaßnahmen kommen bei den Befragten seltener zur Anwendung:

- 41 Prozent der Befragten überprüfen den Sicherheitsstatus der Website, falls personenbezogene Daten angegeben werden müssen.
- 31 Prozent der Befragten lesen die Datenschutzerklärung, bevor persönliche Informationen weitergegeben werden.
- Nur sehr wenige Befragte (15 Prozent) gaben an, bereits einen Antrag gestellt zu haben, um einsehen zu können, welche persönlichen Informationen Onlineplattformen gespeichert haben, um diese dann aktualisieren bzw. löschen zu lassen.

Zur Einordnung der insgesamt hohen Zustimmungswerte für die aufgeführten Schutzmaßnahmen ist zu berücksichtigen, dass die Frequenz, also z. B. in wie vielen Fällen tatsächlich die Datenschutzerklärung gelesen wird, nicht Gegenstand der Fragestellung war. Daraus ergibt sich, dass vielen Verbraucherinnen und Verbrauchern zwar verschiedene Möglichkeiten bekannt sind, selbst einen gewissen Einfluss auf ihre Datensicherheit zu nehmen. Es bleibt an dieser Stelle aber offen, in welcher Regelmäßigkeit oder Konsequenz diese tatsächlich angewendet werden. Auch auf Basis der qualitativen Untersuchungen kann davon ausgegangen werden, dass die Aufmerksamkeit der Verbraucherinnen und Verbraucher im Moment des Onlineshoppings eher auf den genannten Vorteilen von Onlineshopping liegt als bei evtl. Nachteilen (siehe auch Kapitel 4.3.1)

Darüber hinaus sollten die Befragten, die zumindest gelegentlich bei Onlineshops einkaufen, angeben, ob und welche konkreten Schutzmaßnahmen beim Onlineshopping ihnen im Speziellen bekannt sind und welche sie anwenden. Nahezu alle Befragten, die online shoppen, kennen zumindest die folgenden Maßnahmen:

- Verwendung komplexer Passwörter (98 Prozent)
- Verwendung verschiedener Passwörter für unterschiedliche Onlineplattformen (98 Prozent)
- Kauf der Produkte oder Dienstleistungen auf Rechnung (98 Prozent)
- Vermeiden des Anklickens von verdächtigen Webseiten (97 Prozent)
- Ausloggen bei den jeweiligen Onlineplattformen am Ende des digitalen Kaufprozesses (95 Prozent)
- Nutzung eines Passwortmanagers (81 Prozent)
- Nutzung einer Zwei-Faktor-Authentisierung (78 Prozent)

Ein geringerer Anteil an Befragten, die online einkaufen, wendet die betreffenden Maßnahmen auch tatsächlich an:

- Fast neun von zehn Befragten gaben an, komplexe Passwörter zu verwenden.
- 80 Prozent klicken nicht auf verdächtige Websites.
- 79 Prozent loggen sich nach Abschluss des Onlineeinkaufes aus.
- Mehr als drei Viertel der Befragten verwenden mehrere Passwörter für unterschiedliche Onlineplattformen als Maßnahme für eine höhere Datensicherheit bei Onlineeinkäufen und Registrierungen auf Websites.
- Mehr als die Hälfte (64 Prozent) macht vom Kauf auf Rechnung Gebrauch.
- Mehr als die Hälfte (59 Prozent) nutzt die Zwei-Faktor-Authentisierung.
- Einen Passwortmanager nutzen insgesamt nur 27 Prozent der Befragten.

Dabei besteht ein Zusammenhang zwischen der Häufigkeit von Onlineshopping und dem Anwenden verschiedener Schutzmaßnahmen beim Onlineshopping: Personen, die häufiger online einkaufen, nutzen häufiger verschiedene Passwörter für unterschiedliche Onlineshops als Personen, die seltener online einkaufen, ebenso nutzen sie häufiger einen Passwortmanager oder eine zwei-Faktor-Authentisierung (vgl. folgende Abbildung 13).

Abbildung 13 Schutzmaßnahmen Onlineshopping nach Häufigkeit Onlineshopping

Die Ergebnisse der Befragung machen deutlich, dass es eine Diskrepanz zwischen der Kenntnis und Anwendung von Schutzmaßnahmen gibt. Besonders auffällig ist diese bei der Anwendung eines Passwortmanagers, welcher der Mehrheit der Befragten als Schutzmaßnahme bekannt ist (81 Prozent) jedoch nur knapp ein Viertel wenden dies Maßnahme dann auch an (27 Prozent).

Anders verhält es sich bei der Zwei-Faktor-Authentisierung: Interessant ist, dass fast 60 Prozent der Befragten angaben, diese Technik zu nutzen. Für dieses Ausmaß an Nutzungsverbreitung ist die Bekanntheit der Zwei-Faktor-Authentisierung mit 78Prozent erstaunlich gering. Dies legt nahe, dass der Begriff der Zwei-Faktor-Authentisierung zwar einer Mehrheit bekannt ist, jedoch eine starke Minderheit (mehr als 20 Prozent) kann diesen Begriff nur bedingt oder gar nicht einordnen. Dies gilt es in der Kommunikation zu Verbraucherinnen und Verbrauchern zu berücksichtigen.

Außerdem kann die These, dass Verbraucherinnen und Verbraucher sich eher mit entsprechenden Schutzmaßnahmen beschäftigen, wenn sie bereits negative Erfahrungen im Hinblick auf die Datensicherheit beim Onlineshopping gemacht haben, bestätigt werden: So wenden Personen mit negativen Erfahrungen alle Schutzmaßnahmen häufiger an als Personen ohne entsprechende negative Erfahrungen, insbesondere die zwei-Faktor-Authentisierung (68 Prozent der Personen mit negativen Erfahrungen vs. 55 Prozent der Personen ohne negative Erfahrungen) und nicht auf verdächtige Websites zu klicken (85 Prozent der Personen mit negativen Erfahrungen vs. 78 Prozent der Personen ohne negative Erfahrungen). Andererseits legt die hohe Bekanntheit der Schutzmaßnahmen und ihrer Anwendung nahe, dass die These, Verbraucherinnen und Verbraucher resignieren, wenn es zu einem Datenleak-Vorfall kommt, nicht zutreffend ist.

4.3.6 Informations- und Schutzgefühl durch staatliche Institutionen

Wie sehen Verbraucherinnen und Verbraucher die Rolle staatlicher Institutionen zum Thema Datensicherheit beim Onlineshopping? Welche Wahrnehmungen haben sie von staatlichen Institutionen? Wie gut fühlen sich Verbraucherinnen und Verbraucher durch staatliche Institutionen zu dem Thema informiert und geschützt? Inwieweit ist das BSI bekannt und welche Bedeutung haben das BSI bzw. staatliche Institutionen als Informationsquelle und Orientierungshilfe beim Thema Datensicherheit im Onlineshopping aus Sicht der Verbraucherinnen und Verbraucher?

Das Informations- und Schutzgefühl durch staatliche Institutionen hinsichtlich des Themas Datensicherheit beim Onlineshopping ist eher niedrig ausgeprägt (Top-2-Box: gut informiert: 20 Prozent bzw. gut geschützt: 19 Prozent).

Auch Expertinnen und Experten gehen davon aus, dass das BSI nur sehr bedingt eine direkte Anlaufstelle für Verbraucherinnen und Verbraucher darstellt, vor allem mangels Bekanntheit des BSI. Aus der Sicht der Expertinnen und Experten gilt aber das Schaffen einer höheren Aufmerksamkeit für das Thema Datensicherheit in der Bevölkerung vor dem Hintergrund der Kompetenz des BSI als erfolgversprechende Aufgabe. Auch Fortbildungen, Webinare gelten als zielführend, gerade für Shop-Betreiberinnen und -Betreiber, um diese dabei zu unterstützen, einen Webshop nach aktuellen Datensicherheitsrichtlinien aufzubauen.

Jan Mahn vom heise-Verlag sagt hierzu:

> *„Vielleicht müssen wir sagen, das Bundesamt für Sicherheit in der Informationstechnik macht regelmäßig Workshops, so wie das Gesundheitsamt auch Kurse anbietet, in denen Gastronomen lernen, wie man Handhygiene hält. So etwas Ähnliches müsste ich vielleicht als Webshop-Betreiber auch mal nachweisen. Dass mir zumindest mal jemand in so einem BSI-Kurs, online natürlich, an zwei Vormittagen, erzählt hat, dass es dumm ist, alte Software zu betreiben. Und zur Not wird mit schockierenden Horrorbeispielen gearbeitet, die veröffentlicht wurden – prominente Fälle, die wir veröffentlicht haben, waren etwa Datenverluste bei Legoland Deutschland und Buchbinder. Gerne auch Beispiele mit angedrohten oder mit tatsächlichen Strafzahlungen.“*

Die Verbraucherbefragung ergab, dass lediglich etwas mehr als die Hälfte aller Befragten das BSI kennt. Davon hat auch nur ein kleiner Teil (37 Prozent aller Befragten, die das BSI kennen) bereits die Website des BSI schon einmal besucht – bezogen auf die Gesamtheit der Befragten, die generell online einkaufen, sind dies 20 Prozent. Insgesamt gesehen, kann also davon ausgegangen werden, dass das BSI in der breiten Masse der Bevölkerung eher weniger bekannt sind.

Gleichzeitig wünschen sich aber viele Befragte mehr Orientierung, beispielsweise durch ein Siegel, entweder durch eine unabhängige Institution (81 Prozent) oder von staatlicher Seite (68 Prozent), dass die Sicherheit von Onlineshops bewertet und Orientierung bei der Auswahl eines Onlineshops bietet (siehe Kapitel 4.2.2 und 4.3.4). Gerade Personen, die selten online einkaufen, sowie Personen, die generell große Sorgen in Bezug auf die Datensicherheit beim Onlineshopping haben, wünschen sich ein entsprechendes Siegel – entweder von einer unabhängigen dritten Stelle (Personen, die selten online einkaufen: 86 Prozent bzw. Personen mit hohem Besorgnisniveau: 84 Prozent) oder von staatlicher Seite (Personen, die selten online einkaufen: 85 Prozent bzw. Personen mit hohem Besorgnisniveau: 77 Prozent).

Expertinnen und Experten glauben jedoch nur bedingt an die Wirksamkeit von Siegeln, auch wenn dies teilweise expliziter Wunsch der Verbraucherinnen und Verbraucher ist.

> *„Bei Anforderungen im Bereich Zertifikate bin ich immer sehr skeptisch, ob das nicht oft in Geldmacherei abdriftet. Denn insbesondere die Gefahr eines Wildwuchses von Zertifikaten kann die Vertrauenswürdigkeit und damit den Wert von Zertifikaten stark beeinträchtigen. Nutzer werden dazu verleitet zu denken: 'Ach, die haben ja ein Siegel, oder einen blauen Haken - wird schon gut sein.' Das Schutzniveau eines Zertifikates selbst nachzuvollziehen ist für VerbraucherInnen im Alltag letztlich aber auch unzumutbar und unrealistisch.“*
> (Prof. Dr. Timo Jakobi, Technische Hochschule Nürnberg)

5 Zielgruppenspezifische Schlussfolgerungen und Handlungsbedarfe

5.1 Schlussfolgerungen aus der Verbraucherbefragung

5.1.1 Zusammenfassung

Insgesamt 1.018 Verbraucherinnen und Verbraucher wurden im September 2022 im Rahmen einer repräsentativen quantitativen Untersuchung befragt. Zusammenfassend lässt sich festhalten, dass über 90 Prozent der Bevölkerung, die in den letzten zwölf Monaten das Internet genutzt hat, zumindest gelegentlich online einkauft. Davon kaufen rund 19 Prozent ein- oder mehrmals pro Woche im Internet ein, 55 Prozent ein- oder mehrmals pro Monat, 26 Prozent kaufen seltener online ein. Das am häufigsten genutzte Gerät dabei ist das Smartphone (80 Prozent), gefolgt von Laptop (60 Prozent) und PC (48 Prozent) sowie Tablet (40 Prozent). Rund 60 Prozent nutzen außerdem eine App, um im Internet einzukaufen, während 40 Prozent den Onlineshop ausschließlich über den Browser aufrufen. Fast die Hälfte der Befragten (47 Prozent), die nicht online einkaufen, gab an, dass sie Sicherheitsbedenken in Bezug auf ihre persönlichen Daten hätten.

Unabhängig davon, ob man selbst online einkauft oder nicht, gaben insgesamt rund 68 Prozent aller Befragten an, ganz allgemein Bedenken beim Onlineshopping zu haben. Nach konkreten Bedenken gefragt, nannten 61 Prozent das Weiterreichen der persönlichen Daten an Dritte und 50 Prozent das unrechtmäßige Einsehen oder Veröffentlichen der persönlichen Daten. Weitere Bedenken sind, dass das Passwort zum Kundenbereich nicht sicher verschlüsselt wird (37 Prozent), dass es sich bei dem Shop nicht um einen tatsächlich existierenden Onlineshop handelt (36 Prozent) und dass die Ware gar nicht, falsch oder beschädigt ankommt (14 Prozent).

Es zeigt sich, dass Bedenken im Hinblick auf die Datensicherheit beim Onlineshopping bei einem beträchtlichen Anteil der Bevölkerung vorhanden sind. Rund ein Viertel aller Befragten gab an, bereits entsprechende negative Erfahrungen gemacht zu haben. Die häufigsten Reaktionen bei einem (potenziellen) Vorfall in Bezug auf Datensicherheit beim Onlineshopping sind, das Passwort bzw. die Passwörter zu ändern (89 Prozent), Kontakt mit der Shop-Betreiberin bzw. dem Shop-Betreiber aufzunehmen (73 Prozent) oder Accounts, bei denen persönliche Daten hinterlegt sind, zurückzusetzen bzw. zu löschen (66 Prozent). Nur ein geringer Teil der Befragten (ein Prozent) würde sich beim BSI weiter zu dem Vorfall informieren.

Insgesamt besteht große Unsicherheit darüber, welche Auswirkungen das Entwenden bzw. unrechtmäßige Einsehen von Daten für die Betroffenen persönlich hätte: Rund die Hälfte der Befragten wüsste dies nicht genau. Dabei sind 81 Prozent der Befragten, die zumindest gelegentlich im Internet einkaufen, der Meinung, dass das unrechtmäßige Einsehen oder Entwenden der eigenen Daten sehr wahrscheinlich negative Auswirkungen auf sie selbst hätte. Rund die Hälfte derjenigen, die zumindest gelegentlich online einkaufen, wüsste nicht genau, wohin sie sich in einem möglichen Schadensfall mit Fragen wenden sollen, wenn sie erfahren würden, dass bei einem Onlineshop, bei dem sie eingekauft haben bzw. einkaufen, Daten entwendet wurden.

Dabei gab knapp die Hälfte der Befragten an, generelles Interesse am Thema Datensicherheit beim Onlineshopping zu haben (Top-2-Box: 47 Prozent) und sich auch schon einmal zu dem Thema informiert zu haben (52 Prozent der Befragten). 74 Prozent aller Befragten benannten außerdem, was Datensicherheit beim Onlineshopping ihrer Meinung nach bedeutet: In Übereinstimmung mit der Definition des BSI nämlich, dass die persönlichen Daten nicht unrechtmäßig von Dritten eingesehen oder entwendet werden (Mehrfachantwort, gestützte Abfrage). Allerdings muss zur Einordnung dieses Befunds auch berücksichtigt werden, dass die Aspekte „wenn ich Zahlungsdaten hinterlege, werden diese sicher verschlüsselt und ich vor finanziellem Schaden geschützt“ (83 Prozent) und „mein Passwort für den Login zum Kundenbereich eines Onlineshops wird sicher verschlüsselt“ (83 Prozent) aus Sicht der Verbraucherinnen und Verbraucher

ebenfalls zentrale Definitionen des Begriffs Datensicherheit beim Onlineshopping darstellen, gefolgt von weiteren Aspekten die das Weitergeben der Daten an Dritte, das Weitergeben der Einkaufslisten und die Nutzung der persönlichen Daten für Werbezwecke umfassen. Dies zeigt, dass das Begriffsverständnis eher unscharf ist.

Etwas mehr als die Hälfte aller Befragten kennt das BSI zum Zeitpunkt der Befragung, zumindest dem Namen nach. Von staatlicher Seite fühlen sich die Verbraucherinnen und Verbraucher allerdings nur bedingt zum Thema Datensicherheit beim Onlineshopping informiert (Top-2-Box: 20 Prozent) bzw. geschützt (Top-2-Box: 19 Prozent). Die Mehrheit stimmte hier (weniger) zu bzw. war indifferent. Damit besteht ein deutlicher Nachholbedarf, die staatlichen Kommunikationsmaßnahmen zu optimieren und zu erhöhen, um mehr Personen damit zu erreichen.

Maßnahmen, die die Befragten aktuell zum Schutz der eigenen Daten im Internet allgemein anwenden, sind vor allem die Erlaubnisverweigerung personenbezogene Daten zu Werbezwecken zu verwenden (80 Prozent), keine persönlichen Daten (z. B. Kopien vom Führerschein, Personalausweis oder der Gesundheitskarte) in einem Online-Speicher (Cloud) zu speichern (68 Prozent) oder den Zugriff auf geografische Standortdaten zu beschränken (68 Prozent). 64 Prozent der Befragten gaben an, Profilinhalte sozialer Netzwerke nur mit Personen zu teilen, mit denen sie im sozialen Netzwerk verbunden sind. 41 Prozent überprüfen regelmäßig den Sicherheitsstatus der entsprechenden Internetseite, auf der sie personenbezogene Daten hinterlegen müssen. Gut ein Drittel der Befragten (31 Prozent) gab an, sich die Datenschutzerklärung durchzulesen, bevor persönliche Informationen im Internet weitergegeben werden und rund 15 Prozent gaben an, einen Antrag gestellt zu haben, um einsehen zu können, welche persönlichen Informationen Onlineplattformen über sie gespeichert haben, um diese dann aktualisieren bzw. löschen zu lassen.

Schutzmaßnahmen, die konkret beim Onlineshopping zur Anwendung kommen, sind die Nutzung komplexer Passwörter (87 Prozent), keine Klicks auf verdächtige Websites (80 Prozent), Logout bzw. Abmelden über einen entsprechenden Button (79 Prozent), die Nutzung verschiedener Passwörter für unterschiedliche Onlineshops (77 Prozent), Kauf auf Rechnung (64 Prozent), Nutzung von Zwei-Faktor-Authentisierung (59 Prozent) und Nutzung eines Passwortmanagers (27 Prozent). Am unbekanntesten sind generell der Passwortmanager (19 Prozent unbekannt) und die Zwei-Faktor-Authentisierung (22 Prozent unbekannt).

5.1.2 Ableitungen

Die Kernziele des digitalen Verbraucherschutzes erstrecken sich in diesem Kontext im Wesentlichen auf drei Dimensionen, und zwar:

1. **Risikobewusstsein**: Verbraucherinnen und Verbraucher bewerten ihre persönlichen Daten als ein sensibles Gut. Sie sind sich der Risiken und Möglichkeiten eines Verlustes dieser bewusst.
2. **Beurteilungsfähigkeit**: Verbraucherinnen und Verbraucher wissen die Risiken und Möglichkeiten eines Verlustes ihrer persönlichen Daten zu beurteilen. Sie sind sich der potenziell negativen Auswirkungen dessen bewusst.
3. **Lösungskompetenz**: Verbraucherinnen und Verbraucher sind befähigt, den Risiken und Möglichkeiten eines Verlustes ihrer persönlichen Daten entgegenzuwirken. Sie können Maßnahmen ergreifen, um den negativen Auswirkungen zu begegnen.

Im Rahmen der vorliegenden Studie wurde untersucht, inwieweit diese Kernziele bereits erreicht sind, also inwieweit sich Verbraucherinnen und Verbraucher der Risiken beim Onlineshopping im Hinblick auf die Datensicherheit überhaupt bewusst sind, inwiefern sie darüber hinaus in der Lage sind, die Risiken und Möglichkeiten eines Verlusts ihrer persönlichen Daten zu beurteilen, und damit zusammenhängend, ob sie sich der potenziellen negativen Auswirkungen bewusst sind. Schließlich sollte auch untersucht werden, ob sich Verbraucherinnen und Verbraucher in der Lage sehen, dem Verlust ihrer persönlichen Daten entgegenzuwirken bzw. Maßnahmen kennen und ergreifen können, um den negativen Auswirkungen zu

begegnen. An diesen drei Zielen orientiert, lassen sich im Rahmen der nun folgenden drei zusammenfassenden Kapitel mögliche Ableitungen treffen.

5.1.2.1 Risikobewusstsein

Inwiefern ist bei den Verbraucherinnen und Verbrauchern ein Risikobewusstsein im Hinblick auf ihre persönlichen Daten vorhanden, d. h.: Inwiefern sind sie sich der Risiken und Möglichkeiten eines Verlusts ihrer persönlichen Daten bewusst?

Die Studie zeigt, dass sich Verbraucherinnen und Verbraucher nur eingeschränkt bewusst sind, welche Risiken in Bezug auf die Datensicherheit beim Onlineshopping bestehen. So haben lediglich 61 Prozent der Befragten Bedenken, dass ihre persönlichen Daten weitergereicht werden. 50 Prozent haben Bedenken, dass ihre persönlichen Daten von Dritten unrechtmäßig eingesehen oder veröffentlicht werden. 37 Prozent haben Bedenken, dass das Passwort zum Login des Kundenbereichs nicht sicher verschlüsselt wird und 36 Prozent haben Bedenken, dass es sich bei dem Shop nicht um einen tatsächlich existierenden Onlineshop handelt (jeweils Top-2-Box). Insgesamt lediglich 36 Prozent der Befragten machen sich ganz allgemein große Sorgen wegen der Datensicherheit beim Onlineshopping (Top-2-Box).

Daneben erwarten Verbraucherinnen und Verbraucher, dass Onlineshops sich um die Sicherheit ihrer persönlichen Daten kümmern: So gehen 85 Prozent der Befragten davon aus, dass Onlineshops gesetzlich verpflichtet sind, die Sicherheit ihrer persönlichen Daten zu gewährleisten. Sie erwarten, dass Betreiberinnen und Betreiber von Onlineshops über die notwendigen Kenntnisse und Ressourcen zur Sicherstellung der IT-Sicherheit verfügen.

Das Thema Schutz vor finanziellem Schaden ist mehrschichtig. Einerseits ist dieser Punkt ein zentraler Aspekt, der von den Verbraucherinnen und Verbrauchern unter dem übergeordneten Begriff der Datensicherheit beim Onlineshopping gesehen wird (86 Prozent), andererseits ist der Schutz vor finanziellem Schaden für 36 Prozent der Befragten nicht das einzig Relevante. Hinsichtlich der eigenen Risikowahrnehmung geht gut ein Drittel der Befragten davon aus, dass sie bei den von ihnen genutzten Shops eher nicht Opfer eines Datenmissbrauchs werden. Für den Fall, dass doch ein Abfluss von persönlichen Daten erfolgt, gehen über 80 Prozent davon aus, dass dies negative Folgen für sie haben könnte.

Um die Frage zum Risikobewusstsein auf einem übergeordneten Niveau zu beurteilen, wurde ein Index über folgende Fragen gebildet: Q5, Q10, Q12, und Q13 als einfache Summe der Items, die belegt sind (d. h. nicht durchgängig fehlende Werte haben).

Tabelle 6 Items Index Risikobewusstsein

Fragenummer
Q5 Bedenken beim Onlineshopping
..., dass die Ware nicht, falsch oder beschädigt bei mir ankommt.
..., dass es sich nicht um einen tatsächlich existierenden Onlineshop handelt (es den Onlineshop in Wirklichkeit nicht gibt).
..., dass meine persönlichen Daten weitergereicht werden.
..., dass meine persönlichen Daten unrechtmäßig eingesehen oder veröffentlicht werden.
..., dass mein Passwort für den Login zum Kundenbereich eines Onlineshops nicht sicher verschlüsselt wird.
Q10 Grad der Besorgnis beim Onlineshopping
Unabhängig davon, ob Sie selbst online einkaufen, machen Sie sich generell Sorgen im Zusammenhang mit der Sicherheit Ihrer persönlichen Daten beim Onlineshopping, dass sie also von Dritten unrechtmäßig eingesehen oder entwendet werden könnten?
Q12 Wahrscheinlichkeit eines Schadens
Unabhängig davon, ob Sie selbst online einkaufen, für wie wahrscheinlich halten Sie es, dass Ihre persönlichen Daten beim Onlineshopping von Dritten unrechtmäßig eingesehen oder entwendet werden?

Fragenummer
Q13 Einschätzung möglicher Gefahren
Mein Gerät wird mit Schadsoftware infiziert, so dass ich es nicht mehr nutzen kann z. B. Virus, Trojaner.
Mein Passwort zum E-Mailzugang wird gehackt.
Meine Einkaufsliste wird weitergereicht.
Meine persönlichen Daten wie Name, Adresse etc. werden weitergereicht.
Meine Bank- bzw. Kreditkartendaten werden gestohlen.
Auf meinem Gerät werden meine persönlichen Daten verschlüsselt, so dass ich diese nicht mehr nutzen kann.
Meine Daten werden für Identitätsdiebstahl eingesetzt.

Anschließend wurde der Index auf 100 normiert. Insgesamt zeigt sich auch hier, dass ein mittleres Risikobewusstsein vorherrscht: Mittelwert und Median liegen bei 68 und 69 Punkten (Skala: 0-100). Anhand eines Mediansplits (Median: 69) wurden die Personen dann in zwei Gruppen geteilt: Personen mit Indexwert < Median: Geringes Risikobewusstsein (niedriger Risikoindex) und Personen mit Indexwert >= Median: Hohes Risikobewusstsein (hoher Risikoindex).

Auf die Frage, ob sie generell Onlineshopping betreiben, antworteten Personen mit niedrigem Risikoindex eher mit ja als Personen mit hohem Risikoindex (93 Prozent vs. 89 Prozent) (vgl. die folgende Abbildung 14).

Abbildung 14 Onlineshopping ja oder nein nach Risikobewusstsein

Hinsichtlich der Häufigkeit des Onlineshoppings zeigt sich, dass Personen mit hohem Risikoindex deutlich häufiger die Kategorie selten angaben als Personen mit niedrigem Risikoindex (12 Prozent bei Personen mit hohem Risikoindex vs. 5 Prozent bei Personen mit niedrigem Risikoindex) (vgl. folgende Abbildung 15).

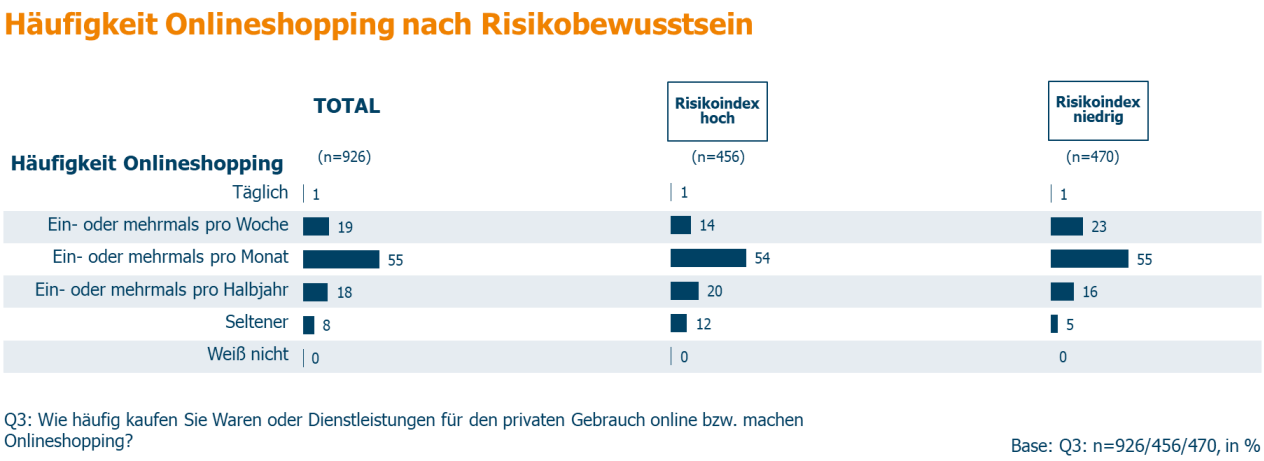


Abbildung 15 Häufigkeit Onlineshopping nach Risikobewusstsein

Auch ist das Interesse an Themen rund um Datensicherheit beim Onlineshopping bei Personen mit einem hohem Risikoindex generell höher ausgeprägt als bei Personen mit niedrigen Risikoindex (54 Prozent bei Personen mit hohem Risikoindex vs. 40 Prozent bei Personen mit niedrigem Risikoindex, jeweils Top-2-Box). Das heißt, dass es einen Zusammenhang gibt zwischen dem Interesse am Thema und dem Bewusstsein hinsichtlich möglicher Risiken. Dementsprechend kann angenommen werden, dass die Steigerung des Interesses am Thema auch mit einer Anhebung des Risikobewusstseins in der Bevölkerung einhergeht.

Einerseits ist der Index für das Risikobewusstsein unter Verbraucherinnen und Verbrauchern eher höher ausgeprägt (Median bei 69 von 100), aber gleichzeitig sind die Bedenken eher verhalten, dass persönliche Daten weitergereicht werden könnten (50 Prozent mit Bedenken, persönliche Daten könnten von Dritten unrechtmäßig eingesehen oder veröffentlich werden). Somit bleibt fraglich, inwieweit die Folgen aus einem Datenabfluss für die Verbraucherinnen und Verbraucher greifbar sind, so dass das Risikobewusstsein geschärft wird. In diesem Zusammenhang muss auch berücksichtigt werden, dass Verbraucherinnen und Verbraucher ein nur ungenaues Verständnis des Datensicherheitsrisikos beim Onlineshopping haben.

Ergänzend zu diesen Ergebnissen der Verbraucherbefragung kann aus den qualitativen Interviews abgeleitet werden, dass die Vorteile wie Bequemlichkeit, Einfachheit oder schnelle Warenverfügbarkeit oft in Konkurrenz zur Umsetzung von bekannten Schutzmaßnahmen stehen und im Zweifel das Vertrauen in den ausgewählten Onlineshop und das Vertrauen in dessen Sicherheitsvorkehrungen überwiegen. Das wahrgenommene Bedrohungspotenzial ist eher auf einem relativ niedrigen Level anzusetzen. Bei einer Minderheit der Befragten, tendenziell diejenigen, die gar nicht oder nur selten online einkaufen, ist das Risikobewusstsein erhöht. Diese reagieren mit Vermeidungsverhalten und unterlassen Onlineshopping eher.

5.1.2.2 Beurteilungsfähigkeit

Inwiefern können Verbraucherinnen und Verbraucher die Risiken und Möglichkeiten eines Verlustes ihrer persönlichen Daten beurteilen und sind sie sich der potenziell negativen Auswirkungen dessen bewusst?

Die Untersuchung legt nahe, dass Verbraucherinnen und Verbraucher nur eingeschränkt urteilsfähig sind, was die Risiken und Möglichkeiten eines Verlusts ihrer persönlichen Daten bedeuten. Sie sind sich der potenziellen negativen Auswirkungen nur bedingt bewusst. Zwar gehen 81 Prozent davon aus, dass ein unrechtmäßiges Einsehen persönlicher Daten negative Auswirkungen hätte, aber nur knapp die Hälfte der Befragten gaben an zu wissen, wohin sie sich bei einem Vorfall in Bezug auf Datensicherheit beim Onlineshopping wenden könnten. Andererseits denkt etwa die Hälfte der Befragten (51 Prozent), dass sie genau wüssten, welche Auswirkungen das Entwenden bzw. unrechtmäßige Einsehen ihrer persönlichen Daten für sie persönlich hätte.

Der Wunsch nach einer Orientierungshilfe ist sehr deutlich: 81 Prozent der Befragten wünschen sich ein Siegel von einer unabhängigen dritten Stelle, welches die Sicherheit von Onlineshops bewertet und Orientierung bei der Auswahl eines Onlineshops bieten könnte. Ebenfalls eine deutliche Mehrheit der Befragten äußerte den Wunsch nach einem entsprechenden Siegel von staatlicher Seite (68 Prozent).

Die Größe des Onlineshops bietet eine gewisse Orientierung und hat Einfluss auf das Vertrauen von Verbraucherinnen und Verbrauchern: Sie vertrauen mehrheitlich großen Onlineshops eher als kleinen (60 Prozent der Befragten).

Ähnlich wie beim Risikobewusstsein wurde auch für die Einschätzung der Beurteilungsfähigkeit ein Index gebildet als Summe aus den Fragen Q8 und Q17 nach dem folgenden Schema, wobei einige Items aufgrund ihrer Relevanz für das Thema nach inhaltlicher Einschätzung des BSI gewichtet wurden (vgl. Tabelle 7):

Tabelle 7 Items Index Beurteilungsfähigkeit

Fragenummer	***Gewichtung mit Faktor***
Q8 Verständnis Datensicherheit	-
Item 2: Meine persönlichen Daten werden nicht von Dritten unrechtmäßig eingesehen oder entwendet.	2
Item 3: Mein Passwort für den Login zum Kundenbereich eines Onlineshops wird sicher verschlüsselt.	1
Item 4: Wenn ich Zahlungsdaten hinterlege, werden diese sicher verschlüsselt und ich vor finanziellem Schaden geschützt.	1
Q17 Einstellungen Datensicherheit und Datenleaks	-
Item 1: Ich gehe davon aus, dass Onlineshops gesetzlich verpflichtet sind, die Sicherheit persönlicher Daten zu gewährleisten.	2
Item 2: Schutz vor finanziellem Schaden ist das Einzige, was mich beim Thema Datensicherheit beim Onlineshopping eigentlich interessiert.	1 (sofern die entgegengesetzte Antwortoption gewählt wurde)
Item 3: Hinsichtlich der Datensicherheit vertraue ich großen Onlineshops oder Plattformen eher als kleinen.	1
Item 6: Ich halte es für unwahrscheinlich, dass bei einem Onlineshop, bei dem ich Kunde bzw. Kundin bin, Daten unrechtmäßig eingesehen und entwendet werden.	2 (sofern die entgegengesetzte Antwortoption gewählt wurde)
Item 7: Ich weiß genau, welche Auswirkungen das Entwenden bzw. unrechtmäßige Einsehen von Daten für mich persönlich hätte.	1
Item 8: Ein unrechtmäßiges Einsehen und Entwenden meiner Daten, hätte sehr wahrscheinlich negative Auswirkungen für mich.	2

Anschließend wurde der Index auf 100 normiert. Insgesamt zeigt sich auch hier, dass ein mittleres Niveau bei der Urteilsfähigkeit vorherrscht: Mittelwert und Median liegen bei 67 und 69 Punkten (Skala: 0-100). Anhand eines Mediansplits (Median: 69) wurden die Personen dann in zwei Gruppen geteilt: Personen mit Indexwert, der unter dem Median liegt und Personen umfasst, die eher ein geringes Urteilsvermögen aufweisen und Personen mit Indexwert, der den Median oder höhere Werte umfasst. Diesen Personen kann ein hohes Urteilsvermögen zugeschrieben werden. Hinsichtlich der Nutzung von Endgeräten bzw. Apps beim Onlineshopping zeigt sich, dass Personen mit hoher Beurteilungsfähigkeit häufiger das Smartphone als das am häufigsten genutzte Gerät für Onlineshopping angaben, als Personen mit niedriger Beurteilungsfähigkeit (42 Prozent vs. 33 Prozent) (vgl. folgende Abbildung 16).

Abbildung 16 Am häufigsten genutztes Gerät beim Onlineshopping nach Beurteilungsfähigkeit

Außerdem nutzen sie häufiger eine App für die betreffenden Onlineshops (63 Prozent vs. 54 Prozent) (vgl. folgende Abbildung 17).

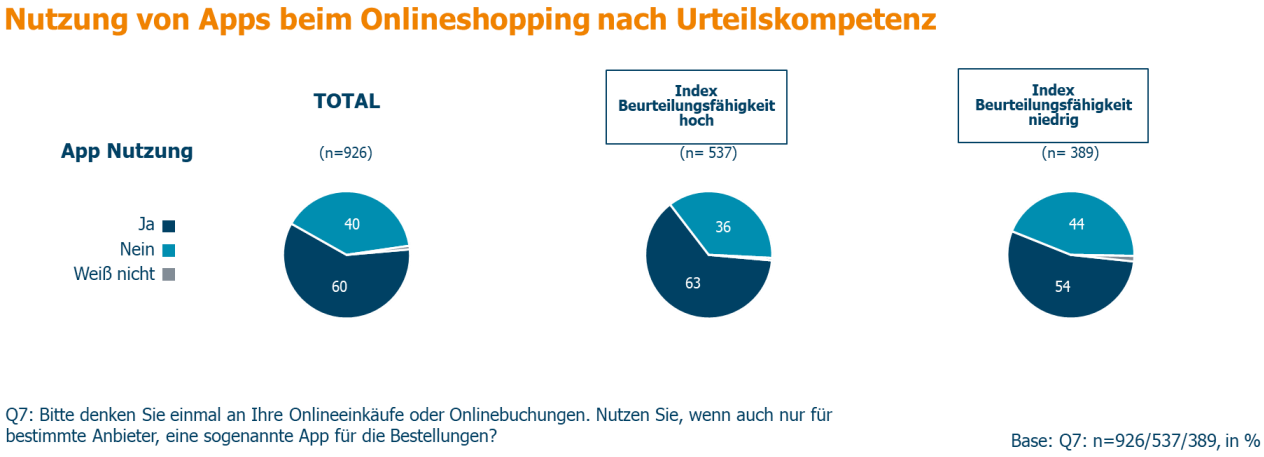


Abbildung 17 Nutzung von Apps beim Onlineshopping nach Beurteilungsfähigkeit

Darüber hinaus zeigt sich, dass Personen mit höherer Beurteilungsfähigkeit weniger Sorgen im Hinblick auf die Datensicherheit beim Onlineshopping haben als Personen mit niedriger Beurteilungsfähigkeit (28 Prozent vs. 41 Prozent, jeweils Top-2-Box). Auch die Einschätzung der Schadenswahrscheinlichkeit ist bei Personen mit hoher Beurteilungsfähigkeit geringer als bei Personen mit niedriger Beurteilungsfähigkeit (29 Prozent vs. 44 Prozent, jeweils Top-2-Box).

Die auf Selbsteinschätzung beruhende Beurteilungsfähigkeit ist eine subjektive Größe und keineswegs objektiv gemessen. Technische Expertinnen und Experten, die mit tiefergehendem Know-how die Komplexität des Themas Datensicherheit beim Onlineshopping sachlicher beurteilen können, konstatieren, dass Verbraucherinnen und Verbrauchern kaum zuzumuten ist, sich beim Einkauf ein objektives Bild von der Datensicherheit eines Shops zu machen. Dies bedeutet, dass hier die eigenen Möglichkeiten als Verbraucherin und Verbraucher oft überschätzt werden.

5.1.2.3 Lösungskompetenz

Inwiefern sind Verbraucherinnen und Verbraucher befähigt, den Risiken und Möglichkeiten eines Verlustes ihrer persönlichen Daten entgegenzuwirken und können sie Maßnahmen ergreifen, um den negativen Auswirkungen zu begegnen?

Wenn Verbraucherinnen und Verbraucher mit einem Datenleak konfrontiert werden, war von Interesse zu untersuchen, ob sie etwas unternehmen würden bzw. unternommen haben, um den negativen Auswirkungen zu begegnen. Insgesamt zeigt sich, dass die große Mehrheit der Befragten etwas unternommen hat bzw. unternehmen würde, wenn es zu einem Datenleak kam bzw. wenn es zu einem Datenleak bei einem Onlineshop, bei dem sie eingekauft haben bzw. einkaufen, kommen würde: Lediglich zwei Prozent der Befragten haben nichts bzw. würden gar nichts tun oder wüssten bzw. wussten nicht was zu tun ist. Etwas höher, aber immer noch sehr gering ist der Anteil derer, die schon einmal negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht haben: Hier gaben neun Prozent an, dass sie gar nichts getan haben bzw. es nicht wissen. Dementsprechend kann die These, dass Verbraucherinnen und Verbraucher resignieren, wenn es zu einem Vorfall in Bezug auf die Datensicherheit kommt, widerlegt werden.

Verbraucherinnen und Verbraucher wenden häufiger Schutzmaßnahmen beim Onlineshopping an, wenn sie schon einmal negative Erfahrungen im Hinblick auf die Datensicherheit beim Onlineshopping gemacht haben. Dies trifft insbesondere auf die Zwei-Faktor-Authentisierung (mit Negativ-Erfahrung: 68 Prozent vs. ohne Negativ-Erfahrung: 55 Prozent) wie auch auf die Maßnahme zu, nicht auf verdächtige Websites zu klicken (mit Negativ-Erfahrung: 85 Prozent vs. ohne Negativ-Erfahrung: 78 Prozent) (vgl. auch Kapitel 4.3.5).

Im Vergleich zu Personen, die sich noch nicht zum Thema Datensicherheit beim Onlineshopping informiert haben, kennen informierte Personen deutlich mehr Schutzmaßnahmen und wenden diese auch an, wie z. B. Nutzung komplexer Passwörter (Informierte: 99 Prozent Kenntnis bzw. 90 Prozent Anwendung vs. Nicht Informierte: 97 Prozent Kenntnis bzw. 81 Prozent Anwendung) oder Logout über einen entsprechenden Button (Informierte: 98 Prozent Kenntnis bzw. 85 Prozent Anwendung vs. Nicht Informierte: 92 Prozent Kenntnis bzw. 71 Prozent Anwendung). Ähnlich verhält es sich bei Personen mit hoher vs. niedriger Selbstwirksamkeitswahrnehmung: Personen, die eine hohe Selbstwirksamkeitswahrnehmung haben, kennen mehr Schutzmaßnahmen beim Onlineshopping und wenden diese auch eher an als Personen mit niedriger Selbstwirksamkeitswahrnehmung (vgl. die folgende Abbildung 18).

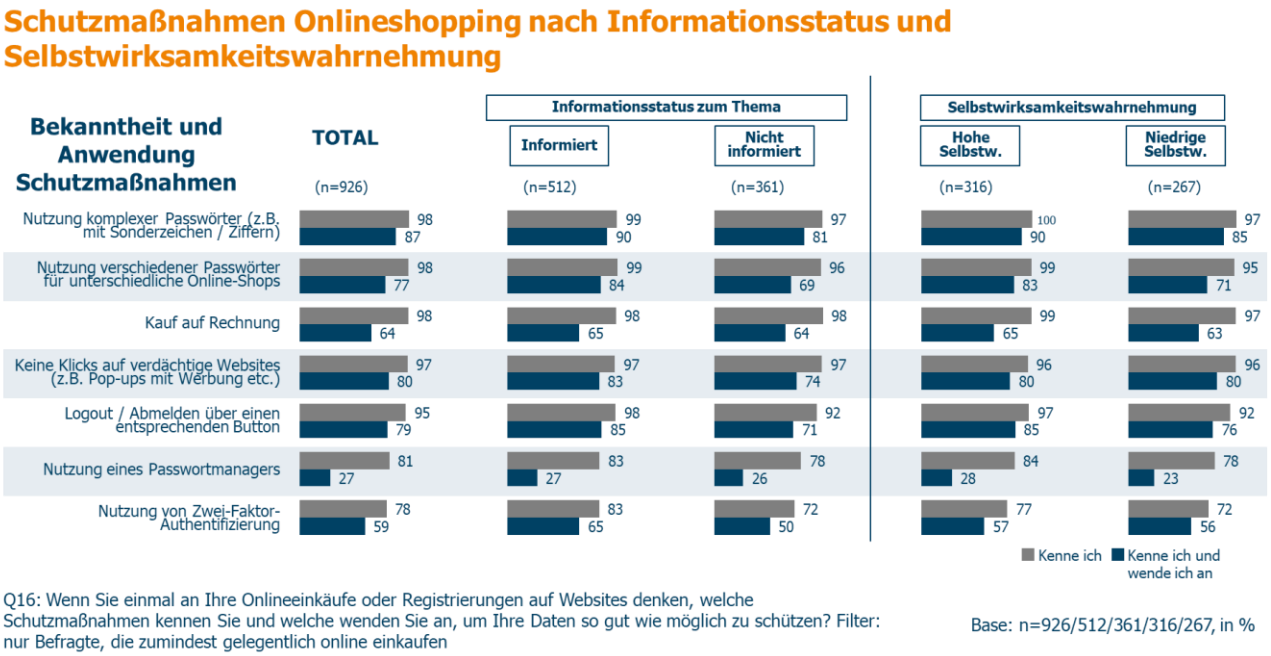


Abbildung 18 Schutzmaßnahmen nach Informationsstatus und Selbstwirksamkeitswahrnehmung

Um die Frage zur Lösungskompetenz noch zusammenfassend zu beurteilen, wurde ein Index über folgende Fragen gebildet: Q15, Q16, Q23 als einfache Summe der Items, die nicht leer sind.

Tabelle 8 Items Index Lösungskompetenz

Fragenummer
Q15 Reaktionen in Bezug auf Datenleak
Ich habe Kontakt mit dem Shop-Betreiber bzw. der Shop-Betreiberin aufgenommen.
Ich habe Kontakt mit der Polizei aufgenommen.
Ich habe Freunde bzw. Bekannte bzw. Familie um Rat gefragt.
Ich habe mich weiter zu dem Vorfall informiert.
Ich habe mein Passwort bzw. meine Passwörter geändert.
Ich habe Accounts, bei denen ich persönliche Daten hinterlegt hatte, zurückgesetzt bzw. gelöscht.
Ich habe etwas anderes unternommen.
Q16 Schutzmaßnahmen beim Onlineshopping (kenne ich und wende ich an)
Nutzung komplexer Passwörter z. B. mit Sonderzeichen bzw. Ziffern
Nutzung verschiedener Passwörter für unterschiedliche Onlineshops
Nutzung eines Passwortmanagers
Nutzung von Zwei-Faktor-Authentifizierung
Kauf auf Rechnung
Logout bzw. Abmelden über einen entsprechenden Button
Keine Klicks auf verdächtige Websites (z. B. Pop-ups mit Werbung oder Gewinnspielen)
Q23 Schutzmaßnahmen im Internet allgemein (habe ich schon ergriffen)
Ich lese aufmerksam die Datenschutzerklärung, bevor ich meine personenbezogenen Daten im Internet weitergebe.
Ich habe die Zugriffsmöglichkeit auf meine geografischen Standortdaten beschränkt.
Nur Personen, mit denen ich in sozialen Netzwerken verbunden bin, können die Inhalte meines Profils sehen.
Ich speichere keine persönlichen Daten (z. B. Kopien vom Führerschein, Personalausweis oder der Gesundheitskarte) in einem Online-Speicher (Cloud).
Ich verweigere regelmäßig meine Zustimmung, dass meine personenbezogenen Daten zu Werbezwecken verwendet werden.
Ich überprüfe regelmäßig den Sicherheitsstatus einer Website, auf der ich meine persönlichen Informationen angeben muss (z. B. Prüfung, ob es sich um eine https- Seite handelt, Sicherheitslogos bzw. Zertifikate).
Ich habe Zugang zu den persönlichen Informationen beantragt, die Onlineplattformen über mich gespeichert haben, um diese Informationen aktualisieren oder löschen zu lassen.

Anschließend wurde der Index auf 100 normiert. Im Vergleich zum Index für das Risikobewusstsein und die Beurteilungsfähigkeit liegt das durchschnittliche Niveau des Index für Lösungskompetenz etwas darunter: Mittelwert und Median liegen bei 59 und 60 Punkten (Skala: 0-100). Anhand eines Mediansplits (Median: 60) wurden die Personen dann in zwei Gruppen geteilt: Personen mit einem Indexwert, der unterhalb des Medians liegt und damit für eine geringere Lösungskompetenz steht und Personen mit einem Indexwert, der gleich dem Median war oder über diesem lag und somit Personen umfasst, die eine höhere Lösungskompetenz aufweisen. Personen mit hoher Lösungskompetenz kaufen generell eher online ein als Personen mit niedriger Lösungskompetenz (99 Prozent vs. 80 Prozent) und interessieren sich häufiger für das Thema Datensicherheit (52 Prozent vs. 41 Prozent).

Unter Berücksichtigung der Tatsache, dass die große Mehrheit der Befragten verschiedene Schutzmaßnahmen beim Onlineshopping kennt und ein Großteil der Befragten diese auch anwendet, widerlegt das die These, dass Verbraucher bei dem Thema gefährdete Datensicherheit resignieren. Andererseits ist das niedrigere Niveau des Lösungskompetenz-Index ein Zeichen für die Notwendigkeit, die Möglichkeit zum Selbstschutz durch ein gezieltes Anheben des Informationsniveaus zu verbessern.

Folgt man dem EPPM-Modell von Witte (1992), sollten mögliche negative Konsequenzen durch Unterlassen von Schutzmaßnahmen auf der Seite der Verbraucherinnen und Verbraucher in Szene gesetzt werden, so dass diese für das Bedrohungspotenzial infolge von Datenleak-Vorfällen bestmöglich sensibilisiert werden. Dass entwendete oder offengelegte Daten eine Gefahr darstellen, erkennt die Mehrheit der Verbraucherinnen und Verbraucher. Dennoch bleibt die Gefahr abstrakt, auch wenn die grundsätzliche Möglichkeit, dass persönliche Zahlungsdaten oder Identitäten gefährdet sind, bekannt ist, scheint der Transfer auf die persönliche Gefährdung oft nicht vollzogen zu werden, so dass auch nur ein gutes Drittel es für wahrscheinlich hält, dass ihre persönlichen Daten beim Onlineshopping von Dritten eingesehen werden. Diese Ambivalenz aus der grundsätzlichen Bekanntheit von Gefahren und dem fehlenden Transfer auf den eigenen Onlineeinkauf kann genutzt werden. Die Aufmerksamkeit von Verbraucherinnen und Verbrauchern kann so durch die an ihrer Lebenswelt ausgerichtete Beschreibung der Gefahr erhöht werden. Bekannte Vorsichtsmaßnahmen können so im Gedächtnis reaktiviert und wieder ins Verhaltensrepertoire aufgenommen werden.

5.2 Schlussfolgerungen aus der Markt- und Schwachstellenanalyse

5.2.1 Marktüberblick und Schwachstellenrecherche

Im Zuge der Marktanalyse konnte ein umfassender Überblick über die auf dem deutschen Markt gängigen Shop-Softwareprodukte und deren Eigenschaften geschaffen werden. 29 Shop-Softwareprodukte wurden erfasst und hinsichtlich der Kategorien „Art der Lösung“ und „Headless-Option“ unterteilt.

Im Anschluss an den Marktüberblick folgte eine Recherche nach bekannten Schwachstellen und Datenleak-Vorfällen, die Auswirkungen auf Verbraucherinnen und Verbraucher aus Deutschland hatten. Insgesamt ermittelte das Projektteam über 400 veröffentlichte Schwachstellen in den letzten fünf Jahren. Hier kristallisierte sich heraus, dass sich die bekannten Schwachstellen vor allem auf Open Source Software beziehen. Aus Sicht des Projektteams lässt sich dies vor allem darauf zurückführen, dass der Quellcode frei zugänglich ist und eine Prüfung daher durch eine Vielzahl von Sicherheitsexpertinnen und -experten erfolgen kann. Bei proprietärer Software, dessen Quellcode nicht offen vorliegt, sind solche Analysen erschwert, daher sind hier deutlich weniger Schwachstellen öffentlich bekannt. Schließlich fand eine Bewertung der veröffentlichten Schwachstellen bezüglich ihrer Relevanz mit Bezug auf eine Offenlegung von Verbraucherdaten statt. Mehr als zwei Drittel der Schwachstellen bringen dabei eine direkte oder potenzielle Gefährdung der Verbraucherdaten mit sich. Dies ist ein sehr hoher Wert und verdeutlicht einmal mehr, wie kritisch Schwachstellen in Shop-Software für Verbraucherdaten sind.

Die Gefährdung der Verbraucherdaten stand ebenfalls im Fokus der Betrachtung von einzelnen Datenleaks. Während der Recherche wurde identifiziert, dass Datenleak-Vorfälle im Onlineshopping in den letzten fünf Jahren stark zugenommen haben. Allein im Jahr 2022 waren zum Zeitpunkt der Recherche acht Vorfälle bekannt. Die meisten dieser Datenleak-Vorfälle ließen sich auf bekannte technische Schwachstellen der eingesetzten Software-Lösungen zurückführen.

5.2.2 Schwachstellenanalysen

Im Zuge der Schwachstellenanalysen wurden zehn zufällig ausgewählte Shop-Softwareprodukte untersucht. Die Ergebnisse hierbei waren sehr heterogen. In einigen Fällen ließen sich nur sehr wenige Schwachstellen identifizieren, dazu mit eher geringen Risikograden. In manchen Fällen jedoch wurden eine Vielzahl von Schwachstellen in den Lösungen identifiziert, auch mit teilweise gravierenden Auswirkungen auf das IT-Sicherheitsniveau.

Die anschließende Kommunikation mit den Herstellern im Zuge des CVD-Prozesses ergab, dass eine sichere Konfiguration der Shop-Software essenziell für die Sicherheit von Verbraucherdaten ist. Einige der gefundenen Schwachstellen waren auf die Webserver zurückzuführen, die für die Prüfungen eingesetzt wurden. Diese wurden, falls vorhanden, nach Anleitung der Hersteller aufgesetzt, konfiguriert und abgesichert. Die dringende Empfehlung lautet daher, dass Hersteller für zukünftige Betreiberinnen und

Betreiber eine Handreichung erstellen. Diese Handreichung sollte eine Anleitung zur sicheren Inbetriebnahme, Konfiguration und Betrieb enthalten. Dies vereinfacht die Konfiguration auf Seiten der Betreiberinnen und Betreiber sehr stark und sorgt für einen höheren und nachhaltigen Schutz der Verbraucherdaten.

Hervorzuheben ist, dass Betreiberinnen und Betreiber in die Lage sein sollten, die Passwortrichtlinie ihres Onlineshops selbst konfigurieren zu können. Das Kundenpasswort bietet Schutz vor unberechtigtem Zugriff. Kann im Shop keine oder nur eine unzureichende Passwortrichtlinie konfiguriert werden, sind die Kundenkonten schlecht geschützt. Eine angemessene Passwortrichtlinie oder gar die Nutzung einer Multi-Faktor-Authentisierung ermöglichen ein hohes Schutzniveau des Kundenkontos.

Weiterhin zu erwähnen ist der Einsatz von JavaScript-Bibliotheken von Drittanbietern. Die eingesetzten Bibliotheken waren häufig verwundbar gegenüber Angriffen oder im schlimmsten Fall bereits seit einiger Zeit vom Hersteller nicht mehr unterstützt und brachten so ein nicht abschätzbares Risiko in die Anwendungen ein. Bei Anwendungen mit Software-Bibliotheken von Drittanbietern ist stets darauf zu achten, dass die neuesten Versionen im Einsatz sind und eine regelmäßige Prüfung auf bekannte Schwachstellen erfolgt.

Die Schwachstellenanalyse wurde mit dem CVD-Prozess abgeschlossen, welcher zum Zeitpunkt dieser Berichtserstellung noch nicht beendet war. Es lässt sich jedoch hervorheben, dass in den meisten Fällen ein Austausch mit den Herstellern auf Augenhöhe möglich war, die Schwachstellen nachgestellt und deren Auswirkungen diskutiert werden konnten. In einigen Fällen standen sehr zeitnah Patches für die gefundenen Schwachstellen zur Verfügung.

5.2.3 Corporate Digital Responsibility (CDR)

Corporate Digital Responsibility (CDR) steht für die Verantwortung von Unternehmen in der digitalen Gesellschaft. Durch den Digitalisierungsschub der letzten Jahre hat die Verantwortung und das Bewusstsein, IT-Sicherheit bereits bei der Entwicklung und Gestaltung digitaler Produkte und Dienstleistungen zu berücksichtigen, zunehmend an Relevanz gewonnen.

Zwischen Anbietern von Shop-Software und den Betreiberinnen und Betreibern von Onlineshops besteht eine enge Kundenbindung bis hin zu einem Lock-in-Effekt. Die Wechselmöglichkeit zu einem anderen Hersteller ist nach der Inbetriebnahme eines Onlineshops begrenzt. Aus Sicht von CDR geht der Vorteil der erhöhten Kundenbindung für die Hersteller von Shop-Software mit einer hohen Verantwortung einher. Daraus folgt, dass die Wahl eines Anbieters bzw. einer Shop-Software eine langfristige strategische Entscheidung ist. Diese Entscheidung hat auch – wie die Ergebnisse der Schwachstellenanalyse verdeutlichte – Auswirkungen auf die IT-Sicherheit der Verbraucherdaten. Betreiberinnen und Betreiber eines Onlineshops müssen in die IT-Sicherheitseigenschaften der von ihnen gewählten Shop-Software vertrauen. Die Verantwortung der Hersteller besteht auch gegenüber Verbraucherinnen und Verbrauchern, denn diese haben nahezu keine Möglichkeit die IT-Sicherheitseigenschaften der eingesetzten Shop-Software zu beurteilen. Schwachstellen in Shop-Softwareprodukten, welche aktiv ausnutzbar sind, haben Auswirkungen auf die Datensicherheit von einer Vielzahl von Verbraucherinnen und Verbrauchern. Dadurch entsteht ein Abhängigkeitsverhältnis beider Gruppen von Anbietern von Shop-Software und macht diese gegenüber Entscheidungen insbesondere zur IT-Sicherheit vulnerabel. Hersteller müssen sich dieser Verantwortung bewusst sein.

Im Rahmen des CVD-Prozesses fanden mehrere Gespräche mit Herstellern statt. Diese stuften einen Teil der identifizierten Schwachstellen aufgrund eines niedrigen oder mittleren Risikograde als nicht relevant ein. In einigen Fällen wurde die Existenz der Schwachstellen auch vollständig angezweifelt, da beispielsweise die Wahrscheinlichkeit der Ausnutzung als sehr gering eingeschätzt wurde. Eine solche Diskussion verdeutlicht die unterschiedlichen Perspektiven auf die gefundenen Schwachstellen. Durch den Dialog mit den Herstellern sollten diese über ihre Verantwortung gegenüber der Sicherheit von Verbraucherdaten sensibilisiert werden. Der Einsatz von verwundbarer oder im schlimmsten Fall nicht mehr unterstützter Software sorgt dafür, dass das Sicherheitsniveau eines Onlineshops in einen undefinierten Zustand

übergeht. Auch eine unzureichende Passwortrichtlinie kann gravierende Folgen für die Sicherheit von Verbraucherdaten haben. Die Betroffenheit der Verbraucherinnen und Verbraucher reicht vom Verlust sensibler Daten, wie z. B. Bank- oder Kreditkartendaten, bis hin zum Identitätsdiebstahl. Doch auch Betreiberinnen und Betreiber eines Onlineshops sind betroffen, beispielsweise infolge betrügerischer Bestellungen oder durch einen Vertrauensverlust von Kundinnen und Kunden.

Darüber hinaus verdeutlichte die Schwachstellenanalyse, dass die Konfigurationsanleitungen einen wichtigen Beitrag für das IT-Sicherheitsniveau darstellen. Einige der identifizierten Schwachstellen ließen sich durch eine bessere Konfigurationsanleitung vermeiden. Geeignete Handlungsempfehlungen für die Installation von Shop-Software, die Berücksichtigung von IT-Sicherheitsaspekten im Entwicklungsprozess sowie ein verantwortungsbewusster Reaktionsprozess im Falle des Auftretens von Schwachstellen leisten einen Beitrag zur Erhöhung der Datensicherheit der Verbraucherdaten im Onlineshopping. Anhand der folgenden Punkte ist vor der Produktauswahl ein verantwortungsvoller Umgang der Hersteller mit dem Thema IT-Sicherheit überprüfbar:

- Welche Aussagen treffen die Hersteller selbst auf ihren Webseiten zum Thema IT-Sicherheit? Hersteller, welche sich nachhaltig um die IT-Sicherheit von Shop-Software sorgen, veröffentlichen zusätzliche Handreichungen, die eine Anleitung zur sicheren Installation und Konfiguration enthalten, wie beispielsweise Informationen über die Konfiguration einer sicheren Passwortrichtlinie oder die Möglichkeit der Implementierung einer Zwei-Faktor-Authentisierung, um einen unberechtigten Zugriff auf Daten zu verhindern.
- Existieren Kontaktwege, wie beispielsweise eine E-Mailadresse, die in Fragen oder bei Auffälligkeiten im Kontext von IT-Sicherheit oder gefundenen Schwachstellen zur Verfügung stehen?
- Veröffentlicht der Hersteller regelmäßige Updates, inklusive Sicherheitsupdates auf seiner Homepage?

Anbietern, welche die Ergebnisse der Schwachstellenanalyse im Rahmen des CVD-Prozesses angenommen und behoben haben, bietet sich die Chance, die eigene Marktpositionierung zu verbessern. Die Umsetzung konkreter IT-Sicherheitsmaßnahmen bilden eine wichtige Grundvoraussetzung für Vertrauen und die Auswahl eines Herstellers, welcher Wert auf eine nachhaltige Verbesserung und Aufrechterhaltung der IT-Sicherheit legt. Kann ein Anbieter dies in seiner Marktansprache positionieren, ist dies ein Gewinn für den Anbieter selbst, aber auch für Betreiberinnen und Betreiber eines Onlineshops und die Sicherheit der Verbraucherdaten.

5.3 Ausblick

Die Digitalisierung bietet für die Gesellschaft neben Veränderungen und Herausforderungen auch viele Vorteile. Hierunter kann sowohl ein digitaler Behördengang, eine virtuelle Finanzberatung oder eben auch das online Einkaufen von Bedarfsgütern fallen. Besteht aber eine wenig ausgeprägte Risikowahrnehmung, dann kann sich dies negativ auf die Nutzung digitaler Angebote auswirken. Vor allem, weil eine niedrige Risikosensibilität die Wahrscheinlichkeit erhöht, selbst Opfer eines Datendiebstahls und -missbrauchs zu werden.

Verbraucherinnen und Verbraucher, die oft online einkaufen, sind sich grundsätzlich der Risiken bewusst. Jedoch zeigt sich, dass diese Risiken im Alltag häufig durch die typischen Vorteile des Onlineshoppings (Einfachheit, Bequemlichkeit etc.) überdeckt werden. Hier ist es wichtig, Risiken und Lösungsmöglichkeiten stärker in den Blick zu rücken.

Die vorliegende Studie zeigt außerdem, dass Verbraucherinnen und Verbraucher eine unscharfe Vorstellung von Datensicherheit beim Onlineshopping haben, die tatsächliche Auswirkung eines Datenabflusses unklar ist und die Frage, an wen man sich im Ernstfall wenden kann, oft unbeantwortet bleibt. Diese Befunde machen deutlich, wie wichtig eine zielgerichtete und zielgruppenorientierte Kommunikation ist, die mit wirksamen Bedrohungsszenarien vorsichtig sensibilisiert und Lösungen anbietet, gleichzeitig aber auch den Begriff Datensicherheit gut eingrenzt und verdeutlicht, was darunter zu verstehen ist.

Es empfiehlt sich, kommunikative Maßnahmen im Hinblick auf die Besorgnis, das Risikobewusstsein und die Beurteilungsfähigkeit zu schärfen. Dies bedeutet, kommunikative Inhalte, Kanäle und deren Gestaltung (Auftritt, Art der Ansprache) nach Möglichkeit nicht pauschal auf alle Verbraucherinnen und Verbraucher anzuwenden, die online einkaufen. Beispiele dafür sind:

- Kommunikative Maßnahmen sollten auch auf die selbst erlebte **Beurteilungsfähigkeit** der Verbraucherinnen und Verbraucher eingehen, sofern diese von der Zielgruppe als hoch eingeschätzt wird. Zielgruppen, die ihre Beurteilungsfähigkeit als eher niedrig einschätzen, sollten jedoch keineswegs demotiviert werden.
- Um die wahrgenommene Sicherheit gerade von Verbraucherinnen und Verbrauchern, die sich eher Sorgen beim Onlineshopping machen, zu stärken, wäre es hilfreich zu betonen, dass das persönliche Risiko durch Achtsamkeit und die Anwendung von Schutzmaßnahmen reduzieren werden kann. Möglichst einfach verständliche Aufklärung und ein Appell, dass man als Verbraucherin und Verbraucher die genannten Gefahren bereits kenne, kann die Aufmerksamkeit auf die Handlungsempfehlungen erhöhen. Da eine Reihe der Vorsichtsmaßnahmen, die auch Expertinnen und Experten empfehlen (z. B. Nutzung eines Passwortmanagers etc.), bei den meisten Verbraucherinnen und Verbrauchern bekannt sind, gilt es die Effektivität der Maßnahmen zu verdeutlichen, um so die Motivation zur Anwendung einfach gehaltener Verhaltensempfehlungen bei Verbraucherinnen und Verbraucher mit niedriger Lösungskompetenz zu erhöhen.
- Personen mit einer **höheren Risikowahrnehmung** oder auch einer **höheren Lösungskompetenz** weisen z. B. ein **deutlich größeres thematisches Interesse** auf. Somit können hier detailliertere Informationen auf eine höhere Akzeptanz und Resonanz stoßen. Wer eine hohe Lösungskompetenz aufweist, informiert sich deutlich häufiger im Internet, beim Verbraucherschutz, bei Behörden allgemein und beim BSI. Informationen dürfen also anspruchsvoller sein.
- Verbraucherinnen und Verbraucher mit einer **niedrigeren Lösungskompetenz** sind häufig älter (60-74 Jahre) und damit im Mix der Informationskanäle häufiger über klassische Medienkanäle (z. B. Zeitung, Fernsehen, Radio) zu erreichen.

Im Sinne des Eingangs angeführten Extended Parallel Process Model (EPPM) lassen sich verschiedene Szenarien ableiten.

- Ausgangspunkt ist das aktuelle, alltägliche Einkaufverhalten im Internet, das von Expertinnen und Experten als in Teilen unreflektiert in Bezug auf Datensicherheit eingeschätzt wird, indem Onlineshopping von starken Motiven wie Einfachheit, Bequemlichkeit, Schnelligkeit dominiert wird. Datensicherheit dürfte beim Onlineshopping für die meisten Verbraucherinnen und Verbraucher definitiv im Hintergrund stehen.
- Dennoch: gefragt nach ihrem Wissen um die Gefährdung von Datensicherheit zeigen sich die Verbraucherinnen und Verbraucher informiert. Hier offenbart sich ambivalentes Verhalten. Verbraucherinnen und Verbraucher sind sich der Risiken im Hinblick auf die Datensicherheit im Onlineshopping bewusst und wenden effektive Maßnahmen an. Dennoch besteht bei einem Großteil der Befragten der Wunsch nach einem Siegel, welches Orientierung bietet.
- Kommunikation, die nun auf Gefahren-Szenarien für die Datensicherheit beim Onlineshopping abstellt, kann z. B. den potenziellen Identitätsdiebstahl oder den Verlust von Zahlungsverkehrsdaten und damit mögliche finanzielle Verluste in den Vordergrund rücken. Die Untersuchung zeigt, dass dies relevante Punkte sind, die Aufmerksamkeit erzeugen können. Ohne ein Mindestmaß an Aufmerksamkeit findet keine Informationsverarbeitung statt.
- Dies kann je nach Zielgruppe zu unterschiedlichen Reaktionen führen:
    - Die Wahrnehmung von Risiken nimmt zu.

- Je nach individueller Ausprägung reagieren Verbraucherinnen und Verbraucher dann mit Angst. Ist die Lösungskompetenz niedrig, kann dies dazu führen, dass im Sinne der Angstkontrolle die Nachricht innerlich zurückgewiesen, also z.B. verdrängt, vergessen oder als irrelevant eingestuft wird.
- Bei einigen dieser Zielgruppe wird sich möglicherweise sogar Vermeidungsverhalten zeigen, also der Verzicht auf oder die Einschränkung von Onlineshopping.
- Daher ist es notwendig, auf Lösungen einzugehen, die den Verbraucherinnen und Verbrauchern bekannt sein könnten. Kommunikation sollte bestärkend sein, gleichsam die Gefahren hinreichend adressieren, und die eigenen Fähigkeiten wie auch das vorhandene Wissen aktivieren.
- Bei einer niedrigeren Lösungskompetenz müssen die vorgeschlagenen Maßnahmen auf möglichst einfach umzusetzende Beispiele beschränkt bleiben.
- Bei einer höheren Lösungskompetenz sollte Kommunikation gezielt an die eigene Kompetenz appellieren, aber dennoch nach wie vor eher einfache Beispiele wählen.

Um nun die richtigen Szenarien für die unterschiedlichen Verbrauchergruppen zu identifizieren, bieten sich eine entlang der Kenntnisse, Bedürfnisse und Selbstwahrnehmung ausgerichtete Segmentierung der Verbraucherinnen und Verbraucher an, die Entwicklung von effizienten Kommunikationsmaßnahmen in einem experimentellen Design und eine Überprüfung ihrer Wirksamkeit. Auf dieser Basis sollte auch der Kanalmix für zukünftige Kommunikationsmaßnahmen in den Blick genommen werden.

Personen, die Onlineshopping vermeiden oder nur selten nutzen, haben deutlich häufiger Bedenken hinsichtlich des Onlineshoppings. Gleichzeitig weist diese Bevölkerungsgruppe tendenziell eine weniger ausgeprägte Beurteilungsfähigkeit und Lösungskompetenz auf und geht seltener davon aus, dass sie selbst dazu beitragen kann, ihre Daten zu schützen. Diese Personengruppe benötigt Informationen in einer für sie verständlichen, nicht zu technischen Sprache, die auf ihre Lebenswelt und Unerfahrenheit in der Nutzung digitaler Angebote zugeschnitten sind.

Um eine Bedürfnissegmentierung zu entwickeln, liefert die vorliegende Studie bereits einige Ansatzpunkte. Diese können sowohl für eine weiterführende qualitative Untersuchung zur Entwicklung von sog. Personas (idealtypische Verbraucherbeschreibungen zur Veranschaulichung von Bedürfnissegmenten) als auch für weitere Untersuchungen zur Identifikation relevanter Szenarien genutzt werden.

Glossar

Tabelle 9: Glossar

Begriff	***Beschreibung***
ADM	Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. / Verband
ADM Dual Frame	Stichprobenbildung mittels Zufallsauswahl aus einer kombinierten Festnetz- und Mobilfunkstichprobe
ADM-Stichprobensystem	Standardisierte Methode der mehrstufigen Ziehung von repräsentativen Stichproben für das Gebiet der Bundesrepublik Deutschland
BIK-Regionsgrößenklassen	Für statistische Analysen wird häufig eine Einteilung von Wohnorten in sieben Größenklassen verwendet. Das BIK-Ortsgrößen- oder Gemeindegrößensystem sind eine bundesweite räumliche Gliederungssystematik, die die Stadt-Umland-Beziehungen auf Gemeindeebene für Ballungsräume, Stadtregionen, Mittel- und Unterzentren darstellt.
Black-Box	Penetrationstest, durchgeführt ohne Kenntnisse der zu prüfenden Umgebung, z. B. nur mit Kenntnis der Adresse eines Zielsystems. Diese Angriffsform versucht die Sichtweise einer externen Angreiferin bzw. eines externen Angreifers ohne Kenntnisse interner Strukturen einzunehmen.
Brute-Force-Angriff	Es handelt sich hierbei um einen Angriff, bei dem beispielsweise versucht wird Benutzernamen oder Passwörter durch wiederholtes und systematisches Ausprobieren zu erraten.
Bug-Bounty-Programm	Ein solches Programm können beispielsweise Hersteller von Softwarelösungen ins Leben rufen. Das Programm bietet Sicherheitsexpertinnen und -experten Prämien für das Entdecken von Schwachstellen oder Fehlern in der Software.
Burp Suite Professional	Prüfwerkzeug mit automatisierten und halb-automatisierten Methoden zur Prüfung von Webanwendungen und Kommunikation.
CATI	(Computer assisted telephone interviews) Telefoninterviews
CAWI	(Computer assisted web interviews) Online-Interviews
Changelogs	Ein Changelog ist ein Änderungsprotokoll. Hersteller können über dieses Protokoll transparent darstellen, welche Änderungen in welcher Version einer Software eingeführt wurden.
Cookie	Ein HTTP-Cookie ist eine Textinformation, die von einer Webanwendung für einen Anwender ausgegeben wird und im Browser der Nutzerin oder des Nutzers gespeichert ist. Das Cookie kann zur Identifizierung oder auch für Webtracking verwendet werden.
Coverage-Probleme	Unter Coverageproblemen sind in diesem Zusammenhang systematische Fehler bzw. Verzerrungen in der Datenbasis zu verstehen, wenn die im Rahmen einer Befragung erreichte Personengruppe in ihrer Struktur nicht der relevanten Grundgesamtheit entspricht.
Cross-Site-Scripting (XSS)	Ein Cross-Site-Scripting beschreibt einen Angriff auf eine Webanwendung, der auf fehlerhafte Validierung von Ein- und Ausgabedaten zurückzuführen ist. Über die Schwachstelle kann es

	Angreiferinnen und Angreifern gelingen, eigenen Code in der Anwendung auszuführen.
Datenleak	Bei einem Datenleak handelt es um einen Vorfall, bei dem sensitive Daten offengelegt werden.
EOL	EOL steht für End of Life und bedeutet, dass die entsprechende Software nicht mehr vom Hersteller unterstützt wird. Für diese Version werden keine Updates und insbesondere keine Sicherheitspatches mehr bereitgestellt.
Heavy-Shopperinnen und -Shopper	Diese sind im Rahmen der Studie definiert über mindestens zwei Online-Einkäufe pro Woche und der Nutzung verschiedener Onlineshops zum Einkaufen, nicht nur ein oder zwei großer Plattformen.
Incentive	Bei einem Incentive in der Sozialforschung handelt es sich um einen Anreiz (oftmals materieller Natur), der geschaffen wird, um die Motivation der Mitwirkenden zu steigern.
Injection	Injection Schwachstellen sind auf Verwundbarkeiten zurückzuführen, bei denen es einer Angreiferin bzw. einem Angreifer gelingt, eigenen Code in der Anwendung einzuschleusen.
LAMP	Es handelt sich hierbei um ein Linuxsystem, auf welchem NGINX/Apache, MySQL und PHP installiert wird, um einen funktionalen Server aufzusetzen
Mixed-Mode-Verfahren	Kombinierte Form der Datenerhebung. In diesem Fall aus Online-Interviews (CAWI) und Telefoninterviews (CATI)
Open Source	Als Open Source wird Software bezeichnet, deren Quelltext öffentlich zugänglich ist und verwendet werden kann.
Penetrationstest	Im Allgemeinen: Sicherheitsüberprüfung einer IT-Umgebung oder Anwendung ohne nähere Spezifikation der Testvorgehensweise.
Qualitative Online-Interviews	Offene Gesprächsführung in längeren Interviews mit Hilfe eines Gesprächsleitfadens durchgeführt.
Quellcode-Analyse	Analyse des Quellcodes einer Anwendung, um diesen einem Sicherheitstest zu unterziehen.
Top-2-Box / Low-2-Box	Mit Hilfe von Top-2-Boxen lassen sich Befragte zusammenfassen, die bei einer Mehrpunkt-Skala die beiden höchsten Antwortoptionen angegeben haben. Analoges gilt für die Low-2-Boxen, bei denen die beiden niedrigsten Antwortoptionen zusammengefasst werden. Auf Basis der Boxen lassen sich entsprechend Aussagen darüber treffen, wie viele Personen die beiden höchsten bzw. niedrigsten Zustimmungswerte angegeben haben.
White-Box	Penetrationstest mit detaillierteren Kenntnissen im Gegensatz zu einem Black-Box-Test. Beispielsweise handelt es sich um einen White-Box-Test, wenn der Quellcode einer Analyse unterzogen wird.

Literaturverzeichnis

Arbeitsgemeinschaft Media-Analyse e.V. und Media-Micro-Census GmbH. 2021. *ma Audio 2021: Die Konvergenzwährung für Radio und Online-Audio – Methodensteckbrief zur Berichtserstattung.* Frankfurt am Main: Arbeitsgemeinschaft Media-Analyse e.V. und Media-Micro-Census GmbH. ISSN 0933-0372, URL:Arbeitsgemeinschaft Media Analyse e.V. (2021). ma Audio 2021

BSI. 2003. *Studie Durchführungskonzept für Penetrationstests.* URL: BSI. (2003). Studie Durchführungskonzept für Penetrationstests.

FIRST.ORG, Inc. *Common Vulnerability Scoring System Calculator*. URL: FIRST.ORG, Inc. Common Vulnerability Scoring System Calculator.

FIRST.ORG, Inc. *Common Vulnerability Scoring System SIG*. URL: FIRST.ORG, Inc. Common Vulnerability Scoring System SIG.

Heise online – c't deckt auf. 2022. *Legoland-Hotelbuchungen der letzten sieben Jahre einsehbar*. URL: Heise online – c't deckt auf. (2022). Legoland-Hotelbuchungen der letzten sieben Jahre einsehbar.

Heise online. 2022. *Brute-Force-Angriff: "Mittlere fünfstellige" Zahl von thalia.de-Konten gehackt.* URL: Heise online. (2022). Brute-Force-Angriff: "Mittlere fünfstellige" Zahl von thalia.de-Konten gehackt.

Heise online. 2022. *Datenleck im Shopsystem von Tuxedo Computers*. URL: Heise online. (2022). Datenleck im Shopsystem von Tuxedo Computers.

MITRE Corporation. *Schwachstellendatenbank*. URL: MITRE Corporation. Schwachstellendatenbank.

NIST National Institute of Standards and Technology. *National Vulnerability Database (NVD) - Schwachstellendatenbank.* URL: NIST National Institute of Standards and Technology. National Vulnerability Database (NVD) - Schwachstellendatenbank.

Open Web Application Security Project. 2020. *Web Security Testing Guide.*URL: Open Web Application Security Project. (2020). Web Security Testing Guide.

Open Web Application Security Project. 2021. *OWASP Top 10.* URL: Open Web Application Security Project. (2021). OWASP Top 10.

Open Web Application Security Project. 2022. *Application Security Verification Standard.* URL: Open Web Application Security Project. (2022). Application Security Verification Standard.

PortSwigger. *Burp Suite Professional.* URL: PortSwigger. Burp Suite Professional.

Statistisches Bundesamt. 2021. *Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien (Mikrozensus-Unterstichprobe zur Internetnutzung).* Fachserie 15 Reihe 4, 14-16. URL: Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien (Mikrozensus-Unterstichprobe zur Internetnutzung) - Fachserie 15 Reihe 4 - 2021 (destatis.de)

The Hacker News. 2022. *Hackers Exploit PrestaShop Zero-Day to Steal Payment Data from Online Stores.* URL: The Hacker News. (2022). Hackers Exploit PrestaShop Zero-Day to Steal Payment Data from Online Stores.

Witte, Kim. 1992. *Putting the fear back into fear appeals: The extended parallel process model.* Communication Monographs, 59(4), 329-349. URL: Witte, K. (1992). Putting the fear back into fear appeals. The extended parallel process model, Communikation Monographs, 59(4)

Anhang

Fragebogen

Screener

Tabelle 10: Frage S1 Screener Last Birthday

THEMA	***Last-Birthday***
FILTER	ALLE
FRAGE	Das Interview dauert etwa 15 Minuten. Die Teilnahme ist selbstverständlich freiwillig und Ihre Angaben werden absolut anonym behandelt. Ich würde zu diesem Zweck gerne mit derjenigen Person in Ihrem Haushalt ein Interview führen, die mindestens 16 Jahre und höchstens 74 Jahre ALT ist UND zuletzt Geburtstag hatte. Sind Sie das oder ist das eine andere Person aus Ihrem Haushalt?
PROG	-

Tabelle 11: Antwort S1 Screener Last Birthday

Antwortmöglichkeiten	***Code***
Zielperson am Telefon (16-74 J. UND zuletzt Geburtstag)	1
Zielperson kommt ans Telefon	2
Nur unter 16 oder über 74-Jährige im Haushalt	-

Tabelle 12: S2 Screener Einleitung

THEMA	Einleitung
FILTER	NUR FÜR CODE 2 AUS S1
FRAGE	PROG: CATI: Guten Tag, hier ist die GIM Dicom in Wiesbaden, mein Name ist ... Wir führen derzeit *im Auftrag des Bundesamts für Sicherheit in der Informationstechnik* bei zufällig ausgewählten Haushalten in Deutschland eine Befragung zu verschiedenen Aspekten der Internetnutzung durch. PROG: CAWI: Hallo und herzlich willkommen zu dieser Umfrage zu verschiedenen Aspekten der Internetnutzung. Vielen Dank, dass Sie uns etwa 15 Minuten Ihrer Zeit schenken, um unsere Studie mit der Beantwortung dieser Fragen zu unterstützen. Alle Informationen und Daten, die Sie mit uns teilen, werden selbstverständlich anonymisiert und streng vertraulich behandelt.
INT	Weitere Informationen bei Bedarf: Der Auftraggeber ist das Bundesamt für Sicherheit in der Informationstechnik. Ihr Haushalt wurde durch eine Zufallsstichprobe ausgewählt

Tabelle 13: Frage S3 Screener Internetzugang

THEMA	Internetzugang
FILTER	ALLE
FRAGE	CATI: Verfügen Sie beruflich oder privat über einen Internetzugang? Bitte denken Sie dabei auch an Ihre mobile Internetnutzung, also z.B. WhatsApp oder ähnliches über Ihr Smartphone. *CAWI: nicht stellen*
PROG	-

Tabelle 14: Antwort S3 Screener Internetzugang

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2 (ENDE)

Tabelle 15: Frage S4 Screener Alter

THEMA	Alter
FILTER	ALLE
FRAGE	Wie alt sind Sie bitte?
PROG	OFFENE ABFRAGE, ZUORDNUNG IM HINTERGRUND Frage für CATI bitte ans Ende zur Statistik nach S4 stellen

Tabelle 16: Antwort S4 Screener Alter

Antwortmöglichkeiten	***Code***
___Jahre	-
keine Angabe	99 (ENDE bei CAWI)

Tabelle 17: Frage S5 Screener Geschlecht

THEMA	Geschlecht
FILTER	ALLE
FRAGE	CAWI: Sind Sie…
PROG	Frage für CATI bitte an Ende zur Statistik VOR D1 stellen mit der Einleitung: Nun sind wir fast am Ende der Befragung. Sie sind …

Tabelle 18: Antwort Frage S5 Screener Geschlecht

Antwortmöglichkeiten	***Code***
Männlich	1
Weiblich	2
Divers	3

Hauptinterview

Tabelle 19: Q1 [F1] Frage Kaufverhalten Onlineshopping

THEMA	Kaufverhalten Onlineshops
FILTER	ALLE
FRAGE	Machen Sie generell Onlineshopping, d.h. kaufen Sie zumindest gelegentlich im Internet bei Online-Shops ein? Damit meinen wir jede Art von Online-Einkauf, wie z.B. Tickets buchen, Lebensmitteleinkauf, Kauf von Kleidung, Büchern, Unterhaltungselektronik etc. Auch Essensbestellungen, die Sie online aufgeben, sind gemeint.
PROG	-

Tabelle 20: Antwort Q1 [F1] Frage Kaufverhalten Onlineshopping

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2

Tabelle 21: Frage Q2 [F2] Gründe gegen Onlineshopping

THEMA	Gründe gegen Onlineshops – Nichtnutzer Onlineshopping
FILTER	NUR FÜR CODE 2 IN Q1
FRAGE	Was sind für Sie persönlich Gründe, lieber in Geschäften vor Ort einzukaufen, anstatt online im Internet? Nur CAWI: Bitte nennen Sie alles, was zutrifft.
PROG	MEHRFACHANTWORT. ROTIEREN AUSSER WEISS NICHT.

Tabelle 22: Antwort Q2 [F2] Gründe gegen Onlineshopping

Antwortmöglichkeiten	***Code***
Ich kaufe nicht im Internet, sondern in Geschäften vor Ort, weil…	1
…ich den lokalen Einzelhandel unterstützen will.	2
…Onlineshopping und der damit zusammenhängende Versand von Paketen schlecht für die Umwelt ist.	3
…meine persönlichen Daten nicht sicher sind beim Onlineshopping.	4
…es keine Beratung beim Onlineshopping gibt.	5
…ich nicht weiß, wie Onlineshopping funktioniert.	6
…ich nicht weiß, wie ich im Internet bezahlen kann.	7
…ich negative Erfahrungen in Bezug auf den Kaufprozess / das Produkt / die Lieferung im Zusammenhang mit Onlineshopping gemacht habe.	8
…ich negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht habe.	9
…ich die Produkte im Geschäft vor Ort direkt ansehen und mitnehmen kann.	10
…ich nutze das Internet gar nicht oder kaum	11
…etwas Anderes, und zwar: _____	12
Weiß nicht	-

Tabelle 23: Frage Q3 [F3] Häufigkeit Onlineshopping

THEMA	Häufigkeit Onlineshopping
FILTER	NICHT FÜR CODE 2 AUS Q1
FRAGE	Wie häufig kaufen Sie Waren oder Dienstleistungen für den privaten Gebrauch online bzw. machen Onlineshopping?
PROG	-

Tabelle 24: Antwort Q3 [F3] Häufigkeit Onlineshopping

Antwortmöglichkeiten	***Code***
Täglich	1
Ein- oder mehrmals pro Woche	2
Ein- oder mehrmals pro Monat	3
Ein- oder mehrmals pro Halbjahr	4
Seltener	5
Weiß nicht	6

Tabelle 25: Frage Q4 [F5] Bedenken Onlineshopping ungestützt

THEMA	Bedenken Onlineshopping – ungestützt
FILTER	ALLE
FRAGE	Onlineshopping umfasst heute sowohl Produkte wie Bücher, Bekleidung, Möbel, Lebensmittel, etc. wie auch Dienstleistungen z.B. Reisen buchen, Versicherungen, etc. und vieles mehr. Unabhängig davon, ob Sie selbst online Waren oder Dienstleistungen einkaufen: Gibt es im Zusammenhang mit Onlineshopping Dinge, bei denen Sie Bedenken haben?
PROG	-

Tabelle 26: Antwort Q4 [F5] Bedenken Onlineshopping ungestützt

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2

Tabelle 27: Frage: Q5 [F6] Bedenken Onlineshopping gestützt

THEMA	Bedenken beim Onlineshopping – gestützt
FILTER	ALLE
FRAGE	CATI: Ich lese Ihnen im Folgenden einige Aspekte im Zusammenhang mit Bedenken, die man beim Onlineshopping haben könnte, vor. Bitte sagen Sie mir, ob Sie persönlich bei den einzelnen Aspekten jeweils eher Bedenken haben oder eher nicht. Bitte verwenden Sie dazu eine Skala von 1-5, wobei eine 1 bedeutet „ich habe keine Bedenken“ und eine 5 bedeutet „ich habe starke Bedenken“. Mit den Werten dazwischen können Sie Ihre Einschätzung abstufen. Wie ist das mit dem Aspekt… CAWI: Unten sehen Sie einige Aspekte im Zusammenhang mit Bedenken, die man beim Onlineshopping haben könnte. Bitte geben Sie an, ob Sie persönlich bei den einzelnen Aspekten jeweils eher Bedenken haben oder eher nicht. Bitte verwenden Sie dazu eine Skala von 1-5, wobei eine 1 bedeutet „ich habe keine Bedenken“ und eine 5 bedeutet „ich habe starke Bedenken“. Mit den Werten dazwischen können Sie Ihre Einschätzung abstufen. Wie ist das mit dem Aspekt…
PROG	BITTE ROTIEREN. ITEM 1-3 IMMER IN DIESER REIHENFOLGE. Inkl. Weiß nicht

Tabelle 28: Antwort Q5 [F6] Bedenken Onlineshopping gestützt

Antwortmöglichkeiten	*Code (Skala 1 bis 5)*
..., dass die Ware **nicht, falsch oder beschädigt** bei mir ankommt	1 – 5, 99 (weiß nicht)
..., dass es sich **nicht** um einen **tatsächlich existierenden Online-Shop** handelt (es den Online-Shop in Wirklichkeit nicht gibt)	1 – 5, 99 (weiß nicht)
..., dass **meine persönlichen Daten weitergereicht werden.**	1 – 5, 99 (weiß nicht)
..., dass meine persönlichen Daten **unrechtmäßig eingesehen oder veröffentlicht** werden	1 – 5, 99 (weiß nicht)
..., dass **mein Passwort für den Login** zum Kundenbereich eines Online-Shops **nicht sicher verschlüsselt** wird	1 – 5, 99 (weiß nicht)

Tabelle 29: Frage Q6 [F8] Nutzung Endgeräte Onlineshopping

THEMA	Endgeräte Onlineshopping
FILTER	NICHT FÜR CODE 2 IN Q1
FRAGE	Welches der folgenden Geräte nutzen Sie am häufigsten für Ihre Onlineeinkäufe, welches am zweithäufigsten und so weiter. Zusatztext bei [F8_1] Item 1: „am häufigsten“ [F8_2] Item 2: „am zweithäufigsten“ [F8_3] Item 3: „am dritthäufigsten“ [F8_4] Item 4: „am vierthäufigsten“
PROG	RANKING. MIND. 1 NENNUNG, ALLE KÖNNEN GERANKT WERDEN. ROTIEREN

Tabelle 30: Antwort Q6 [F8] Bedenken Onlineshopping gestützt

Antwortmöglichkeiten	*Code*
PC	1
Laptop	2
Smartphone	3
Tablet	4
Nutze kein weiteres Gerät	5

Tabelle 31: Frage Q7 [F9] Nutzung Apps Onlineshopping

THEMA	Nutzung Apps beim Onlineshopping
FILTER	Nur wenn Q1=1
FRAGE	Bitte denken Sie einmal an Ihre Onlineeinkäufe oder Onlinebuchungen. Nutzen Sie, wenn auch nur für bestimmte Anbieter, eine sogenannte App für die Bestellungen? [INT: NUR BEI SCHWIERIGKEITEN ERKLÄREN] Mit App ist dabei folgendes gemeint: Viele Anbieter bieten sogenannte Apps an, um in dem jeweiligen Onlinegeschäft einzukaufen. Auf dem Smartphone sind Apps als "Kachel" oder Symbol dargestellt und Sie gelangen darüber direkt in das Geschäft/Store

Tabelle 32: Antwort Q7 [F9] Nutzung Apps Onlineshopping

Antwortmöglichkeiten	*Code*
Ja	1
Nein	2
Weiß nicht	9

Tabelle 33: Frage Q8 [F10] Datensicherheit Onlineshopping

THEMA	Verständnis Datensicherheit beim Onlineshopping
FILTER	ALLE
FRAGE	Was bedeutet Ihrer Meinung nach Datensicherheit beim Onlineshopping, also Datensicherheit beim Einkaufen im Internet? Ich lese Ihnen mögliche Aspekte vor, bitte sagen Sie mir welche Ihrer Meinung nach zutreffen. CAWI: Was bedeutet Ihrer Meinung nach Datensicherheit beim Onlineshopping, also Datensicherheit beim Einkaufen im Internet? Welche der nachfolgenden Aspekte treffen Ihrer Meinung nach zu.
PROG	ROTIEREN

Tabelle 34: Antwort Q8 [F10] Datensicherheit Onlineshopping

Antwortmöglichkeiten	***Code***
Meine persönlichen Daten werden nicht an Dritte weitergegeben.	1
Meine persönlichen Daten werden nicht von Dritten unrechtmäßig eingesehen oder entwendet.	2
Mein Passwort für den Login zum Kundenbereich eines Online-Shops wird sicher verschlüsselt.	3
Wenn ich Zahlungsdaten hinterlege, werden diese sicher verschlüsselt und ich vor finanziellem Schaden geschützt.	4
Informationen über meine Einkäufe werden nicht für Werbung benutzt	5
Die Liste meiner Einkäufe wird nicht an Dritte weitergegeben.	6
Nichts davon [PROG: Optisch absetzen, IMMER AN DIESER STELLE]	7
Weiß nicht [PROG: EXKL., IMMER AN DIESER STELLE]	99

Tabelle 35: Q9 [F11] Definition Datensicherheit

THEMA	Definition Datensicherheit beim Onlineshopping
FILTER	ALLE
FRAGE	Damit alle Teilnehmer für die folgenden Fragen die gleiche Definition zum Thema Datensicherheit gehört haben, folgt hier nun eine allgemeine Definition: Unter Datensicherheit beim Onlineshopping wird allgemein verstanden, dass die persönlichen Daten nicht von Dritten unrechtmäßig eingesehen oder entwendet werden. PROG: CATI: Bitte denken Sie bei der Beantwortung der folgenden Fragen an diese Definition. Ich kann Sie Ihnen gern jederzeit wieder vorlesen. PROG: CAWI: Bitte denken Sie bei der Beantwortung der folgenden Fragen an diese Definition. Sie können sich diese immer wieder einblenden lassen.
PROG	Mouseover Definition „Datensicherheit: Unter Datensicherheit beim Onlineshopping wird allgemein verstanden, dass die persönlichen Daten nicht von Dritten unrechtmäßig eingesehen oder entwendet werden.“

Tabelle 36: Frage Q10 [F12] Sorgen Datensicherheit Onlineshopping

THEMA	Sorgen wegen Datensicherheit im Internet
FILTER	ALLE
FRAGE	Unabhängig davon, ob Sie selbst online einkaufen, machen Sie sich generell Sorgen im Zusammenhang mit der Sicherheit Ihrer persönlichen Daten beim Onlineshopping, dass sie also von Dritten unrechtmäßig eingesehen oder entwendet werden könnten? Verwenden Sie dazu bitte die Skala von 1 „gar keine Sorgen“ bis 5 „große Sorgen“. Mit den Werten dazwischen können Sie Ihre Meinung beliebig abstufen.
PROG	Inkl. Weiß nicht Mouseover Definition „Datensicherheit: Unter Datensicherheit beim Onlineshopping wird allgemein verstanden, dass die persönlichen Daten nicht von Dritten unrechtmäßig eingesehen oder entwendet werden.“

Tabelle 37: Antwort Q10 [F12] Sorgen Datensicherheit Onlineshopping

Antwortmöglichkeiten	***Code***
1 = gar keine Sorgen	1
2	2
3	3
4	4
5 = große Sorgen	5
Weiß nicht	6

Tabelle 38: Frage Q11 [F13] Thematisches Interesse Datensicherheit Onlineshopping

THEMA	Thematisches Interesse
FILTER	ALLE
FRAGE	Unabhängig davon, ob Sie selbst online einkaufen, wie sehr interessieren Sie sich für Themen rund um Datensicherheit beim Onlineshopping? Verwenden Sie dazu bitte die Skala von 1 “überhaupt nicht interessiert“ bis 5 “sehr interessiert“. Mit den Werten dazwischen können Sie Ihre Meinung beliebig abstufen.
PROG	Inkl. Weiß nicht Mouseover Definition „Datensicherheit: Unter Datensicherheit beim Onlineshopping wird allgemein verstanden, dass die persönlichen Daten nicht von Dritten unrechtmäßig eingesehen oder entwendet werden.“

Tabelle 39: Antwort Q11 [F13] Thematisches Interesse Datensicherheit Onlineshopping

Antwortmöglichkeiten	***Code***
1 = überhaupt nicht interessiert	1
2	2
3	3
4	4
5 = sehr interessiert	5

Tabelle 40: Frage Q12 [F15] Wahrscheinlichkeit Schadensfall

THEMA	Wahrscheinlichkeit Schadenfall
FILTER	ALLE
FRAGE	Unabhängig davon, ob Sie selbst online einkaufen, für wie wahrscheinlich halten Sie es, dass Ihre persönlichen Daten beim Onlineshopping von Dritten unrechtmäßig eingesehen oder entwendet werden? Antworten Sie bitte auf einer Skala von 1 bis 5, wobei 1 “sehr unwahrscheinlich” und 5 “sehr wahrscheinlich” bedeutet. Mit den Werten dazwischen können Sie Ihr Urteil abstufen.
PROG	Inkl. Weiß nicht

Tabelle 41: Antwort Q12 [F15] Wahrscheinlichkeit Schadensfall

Antwortmöglichkeiten	***Code***
1 = sehr unwahrscheinlich	1
2	2
3	3
4	4
5 = sehr wahrscheinlich	5

Tabelle 42: Frage Q13 [F17] Gefahren im Internet allgemein

THEMA	Relation Gefahren im Internet allgemein vs. Datensicherheit
FILTER	ALLE
FRAGE	CATI: Ich lese Ihnen nun einige Aspekte zu möglichen Gefahren in Zusammenhang mit der Nutzung des Internets vor. Bitte sagen Sie mir zu jedem Aspekt, ob Sie diesen für sich persönlich als eher gefährlich oder eher nicht gefährlich einschätzen. Bitte verwenden Sie dazu eine Skala von 1-5, wobei eine 1 bedeutet „ist für mich nicht gefährlich“ und eine 5 bedeutet „ist für mich sehr gefährlich“. Mit den Werten dazwischen können Sie Ihre Einschätzung abstufen. CAWI: Sie sehen nun einige Aspekte zu möglichen Gefahren in Zusammenhang mit der Nutzung des Internets. Bitte geben Sie zu jedem Aspekt an, ob Sie diesen für sich persönlich als eher gefährlich oder eher nicht gefährlich einschätzen. Bitte verwenden Sie dazu eine Skala von 1-5, wobei eine 1 bedeutet „ist für mich nicht gefährlich“ und eine 5 bedeutet „ist für mich sehr gefährlich“. Mit den Werten dazwischen können Sie Ihre Einschätzung abstufen.
PROG	ROTIEREN. Inkl. Weiß nicht

Tabelle 43: Antwort Q13 [F17] Gefahren im Internet allgemein

Antwortmöglichkeiten	***Code (Skala 1- 5)***
Mein Gerät wird mit Schadsoftware infiziert, so dass ich es nicht mehr nutzen kann z.B. Virus, Trojaner.	1 – 5, 6 (weiß nicht)
Mein Passwort zum E-Mailzugang wird gehackt.	1 – 5, 6 (weiß nicht)
Meine Einkaufsliste wird weitergereicht (MOUSEOVER Einkaufsliste: Interviewer auf Nachfrage: die Übersicht über die Produkte, die von mir in einem Online-Shop gekauft wurden)	1 – 5, 6 (weiß nicht)
Meine persönlichen Daten wie Name, Adresse etc. werden weitergereicht.	1 – 5, 6 (weiß nicht)
Meine Bank-/Kreditkartendaten werden gestohlen.	1 – 5, 6 (weiß nicht)

Antwortmöglichkeiten	*Code (Skala 1- 5)*
Auf meinem Gerät werden meine persönlichen Daten verschlüsselt, so dass ich diese nicht mehr nutzen kann.	1 – 5, 6 (weiß nicht)
Meine Daten werden für Identitätsdiebstahl eingesetzt.	1 – 5, 6 (weiß nicht)

Tabelle 44: Frage Q14 [F18] Negative Erfahrungen Datensicherheit Onlineshopping

THEMA	Online-Shopper: Negative Erfahrungen in Bezug auf Datensicherheit bei Online-Shops
FILTER	ALLE
FRAGE	Haben Sie schon einmal negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht, dass also Ihre persönlichen Daten von Dritten unrechtmäßig eingesehen oder gestohlen wurden?
PROG	-

Tabelle 45: Antwort Q14 [F18] Negative Erfahrungen Datensicherheit Onlineshopping

Antwortmöglichkeiten	*Code*
Ja	1
Nein	2

Tabelle 46: Frage Q15 [F19] Reaktionen Vorfall

THEMA	Reaktionen auf Vorfall in Bezug auf Datensicherheit
FILTER	ALLE
FRAGE	NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Sie haben angegeben, dass Sie schon einmal negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping gemacht haben. Was haben Sie dann getan? ALLE ANDEREN: Wenn Sie sich vorstellen, dass Sie negative Erfahrungen in Bezug auf die Datensicherheit beim Onlineshopping machen würden. Was würden Sie dann tun?
PROG	IMMER IN DIESER REIHENFOLGE

Tabelle 47: Antwort Q15 [F19] Reaktionen Vorfall

Antwortmöglichkeiten	***Code***
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe Kontakt mit dem Shop-Betreiber / der Shop-Betreiberin aufgenommen. ALLE ANDEREN: Ich würde Kontakt mit dem Shop-Betreiber / der Shop-Betreiberin aufnehmen.	1
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe Kontakt mit der Polizei aufgenommen. ALLE ANDEREN: Ich würde mit der Polizei Kontakt aufnehmen.	2
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe Freunde / Bekannte / Familie um Rat gefragt. ALLE ANDEREN: Ich würde Freunde / Bekannte / Familie um Rat fragen.	3
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe mich weiter zu dem Vorfall informiert, und zwar bei: [PROG, OFFENES TEXTFELD] _____. ALLE ANDEREN: Ich würde mich weiter zu dem Vorfall informieren, und zwar bei: [PROG, OFFENES TEXTFELD] ____.	4
NUR FÜR CODE 1 IN VORFRAGE ODER CODE 8 IN Q2: Ich habe mein Passwort/meine Passwörter geändert. ALLE ANDEREN: Ich würde mein Passwort/meine Passwörter ändern.	5
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe Accounts, bei denen ich persönliche Daten hinterlegt hatte, zurückgesetzt / gelöscht. ALLE ANDEREN: Ich würde Accounts, bei denen ich persönliche Daten hinterlegt hatte, zurücksetzen / löschen.	6
Etwas anderes, und zwar: _____ [PROG: IMMER AN DIESER STELLE]	7
NUR FÜR CODE 1 IN Q14 ODER CODE 8 IN Q2: Ich habe gar nichts unternommen. ALLE ANDEREN: Ich würde gar nichts unternehmen.	8
Weiß nicht [PROG: EXKL., IMMER AN DIESER STELLE]	9

Tabelle 48: Frage Q16 [F21] Schutzmaßnahmen Onlineshopping

THEMA	Schutzmaßnahmen Onlineshopping
FILTER	NICHT FÜR CODE 2 AUS Q1
FRAGE	CATI: Wenn Sie einmal an Ihre Onlineeinkäufe oder Registrierungen auf Websites denken, welche Schutzmaßnahmen kennen Sie und welche wenden Sie an, um Ihre Daten so gut wie möglich zu schützen? Ich lese Ihnen nacheinander mögliche Schutzmaßnahmen vor. Bitte sagen Sie mir jeweils, ob Sie diese kennen oder auch anwenden. CAWI: Wenn Sie einmal an Ihre Onlineeinkäufe oder Registrierungen auf Websites denken, welche Schutzmaßnahmen kennen Sie und welche wenden Sie an, um Ihre Daten so gut wie möglich zu schützen? Bitte nennen Sie alles, was zutrifft.
PROG	EINFACHANTWORT PRO ZEILE KENNE / WENDE AN. ROTIEREN, [MOUSEOVER BROWSER: Ich tippe die Adresse des Online-Shops in der Adresszeile ein oder rufe einen entsprechenden Link auf]

Tabelle 49: Antwort Q16 [F21] Schutzmaßnahmen Onlineshopping

Antwortmöglichkeiten	***Code (Kenne ich nicht = 1, Kenne ich = 2, Kenne ich und wende ich an = 3)***
Nutzung komplexer Passwörter z.B. mit Sonderzeichen / Ziffern	1 - 3
Nutzung verschiedener Passwörter für unterschiedliche Online-Shops	1 - 3
Nutzung eines Passwortmanagers	1 - 3
Nutzung von Zwei-Faktor-Authentifizierung	1 - 3
Kauf auf Rechnung	1 - 3
Logout/ Abmelden über einen entsprechenden Button	1 - 3
Keine Klicks auf verdächtige Websites (z.B. Pop-ups mit Werbung oder Gewinnspielen)	1 - 3

Tabelle 50: Frage Q17 [F22] Einstellungen Datensicherheit und Datenleak-Vorfall

THEMA	Einstellungen Datensicherheit & Datenleak
FILTER	CODE 2 AUS Q1 BEKOMMT NUR Item 1+2+7+8, DER REST BEKOMMT ALLES
QUESTION	Es folgen nun einige Aussagen zum Thema Datensicherheit beim Onlineshopping. Dabei geht es auch um das Thema Sicherheitslücken bei der Übertragung von Daten, also wenn private Daten unrechtmäßig eingesehen oder entwendet werden. Treffen die folgenden Aussagen aus Ihrer Sicht zu oder nicht? Bitte antworten Sie jeweils mit „Ja“ oder „Nein“.
PROG	INNERHALB DER BLÖCKE ROTIEREN. 5 IMMER NACH 4

Tabelle 51: Antwort Q17 [F22] Einstellungen Datensicherheit und Datenleak-Vorfall

Antwortmöglichkeiten	***Code (ja = 1, nein = 2)***
Ich gehe davon aus, dass Online-Shops gesetzlich verpflichtet sind, die Sicherheit persönlicher Daten zu gewährleisten.	1 - 2
Schutz vor finanziellem Schaden ist **das Einzige**, was mich beim Thema Datensicherheit beim Onlineshopping eigentlich interessiert.	1 - 2

Antwortmöglichkeiten	*Code (ja = 1, nein = 2)*
Hinsichtlich der Datensicherheit vertraue ich großen Online-Shops oder Plattformen eher als kleinen	1 - 2
Ich wünsche mir ein Siegel von einer unabhängigen dritten Stelle wie z. B. TÜV oder Trusted Shops, welches die Sicherheit von Online-Shops bewertet und mir Orientierung bei der Auswahl eines Online-Shops bietet	1 - 2
Ich wünsche mir ein **Siegel von staatlicher Seite,** dass die Sicherheit von Online-Shops bewertet und mir Orientierung bei der Auswahl eines Online-Shops bietet	1 - 2
Ich halte es für unwahrscheinlich, dass bei einem Online-Shop, bei dem ich Kunde / Kundin bin, Daten unrechtmäßig eingesehen und entwendet werden.	1 - 2
Ich weiß genau, welche Auswirkungen das Entwenden bzw. unrechtmäßige Einsehen von Daten für mich persönlich hätte.	1 - 2
Ein unrechtmäßiges Einsehen und Entwenden meiner Daten, hätte sehr wahrscheinlich negative Auswirkungen für mich.	1 - 2
Wenn ich erfahren würde, dass bei einem Online-Shop, bei dem ich Kunde / Kundin bin, Daten entwendet wurden, wüsste ich, wohin ich mich mit meinen Fragen wenden kann.	1 - 2

Tabelle 52: Frage Q18 [F24] Informations- und Schutzempfinden

THEMA	Informations- und Schutzgefühl
FILTER	ALLE
QUESTION	Wie gut fühlen Sie sich durch staatliche Institutionen und Institutionen des Verbraucherschutzes zum Thema Datensicherheit beim Onlineshopping informiert bzw. geschützt? Verwenden Sie dazu bitte die Skala von 1 “überhaupt nicht gut“ bis 5 “sehr gut“. Mit den Werten dazwischen können Sie Ihre Meinung beliebig abstufen.
PROG	Mouseover Definition „Datensicherheit: Unter Datensicherheit beim Onlineshopping wird allgemein verstanden, dass die persönlichen Daten nicht von Dritten unrechtmäßig eingesehen oder entwendet werden.“

Tabelle 53: Antwort Q18 [F24] Informations- und Schutzempfinden

Antwortmöglichkeiten	*Code (überhaupt nicht gut = 1, sehr gut = 5)*
Informiert	1 – 5
Geschützt	1 – 5

Tabelle 54: Frage Q19 [F25] Bekanntheit BSI

THEMA	Bekanntheit BSI
FILTER	ALLE
FRAGE	Kennen Sie das Bundesamt für Sicherheit in der Informationstechnik (BSI), wenn auch nur dem Namen nach?
PROG	-

Tabelle 55: Antwort Q19 [F25] Bekanntheit BSI

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2

Tabelle 56: Frage Q20 [F26] Website BSI

THEMA	Website BSI
FILTER	NUR FÜR CODE 1 IN 19
FRAGE	Haben Sie die Website des Bundesamtes für Sicherheit in der Informationstechnik (BSI) schon einmal besucht?
PROG	-

Tabelle 57: Antwort Q20 [F26] Website BSI

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2
Weiß nicht	9

Tabelle 58: Frage Q21a [F27] Informationen Datensicherheit

THEMA	Informationen Ja/Nein
FILTER	ALLE
FRAGE	Haben Sie sich schon einmal zum Thema Datensicherheit beim Onlineshopping informiert?
PROG	-

Tabelle 59: Antwort Q21a [F27] Informationen Datensicherheit

Antwortmöglichkeiten	***Code***
Ja	1
Nein	2
Weiß nicht	9

Tabelle 60: Frage Q21 [F27A] Informationskanäle Datensicherheit

THEMA	Informationen
FILTER	NUR FÜR CODE 1 IN Q21a
FRAGE	Wo haben Sie sich schon einmal zum Thema Datensicherheit beim Onlineshopping informiert? War das...
PROG	MEHRFACHANTWORT. ROTIEREN

Tabelle 61: Antwort Q21 [F27A] Informationskanäle Datensicherheit

Antwortmöglichkeiten	***Code***
Im Internet allgemein (z.B. über Suchmaschinen)	1
In soziale Medien wie Facebook, Instagram, TikTok, etc.	2
Über Video-/Streaming-Plattformen (z. B. YouTube, Netflix, Amazon Prime)	3
In speziellen Blogs / Foren im Internet, Podcasts	4
Bei Freunden, Familie, Kollegen	5
In Tages- oder Wochenzeitungen (INT bei Nachfragen: egal, ob als ePaper, Nachrichten in der App der Zeitung oder über die gedruckte Ausgabe der Zeitung)	6
Im Fernsehen/in Mediatheken	7
Im Radio/Webradio	8
Beim Bundesamt für Sicherheit in der Informationstechnik (BSI)	9
Bei Behörden allgemein	10
Bei der Verbraucherzentrale / beim Verbraucherschutz	11
Weiß nicht [PROG: EXKLUSIV, IMMER AN DIESER STELLE]	14

Tabelle 62: Frage Q22 [F28] Einstellungen Datensicherheit

THEMA	Einstellungen
FILTER	ALLE
FRAGE	Wenn Sie nun einmal alles zusammennehmen, was Sie heute über Datensicherheit beim Onlineshopping wissen, inwiefern stimmen Sie den folgenden Aussagen zu? Verwenden Sie dazu bitte die Skala von 1 „stimme überhaupt nicht zu“ bis 5 „stimme voll und ganz zu“. Mit den Werten dazwischen können Sie Ihre Meinung beliebig abstufen.
PROG	-

Tabelle 63: Antwort Q22 [F28] Einstellungen Datensicherheit

Antwortmöglichkeiten	***Code (stimme überhaupt nicht zu = 1, stimme voll und ganz zu = 5)***
Beim Onlineshopping kann man selbst dafür sorgen, dass die persönlichen Daten sicher sind.	1 – 5
Wenn meine Daten bei einem Online-Shop in dem ich einkaufe, entwendet werden, kann ich nichts tun, um die Folgen für mich abzumildern.	1 – 5
Ich wurde schon öfter mit Problemen bei der Datensicherheit meiner persönlichen Daten im Internet konfrontiert.	1 – 5
Ich bin in Bezug auf meine persönlichen Daten generell sehr vorsichtig.	1 – 5

Tabelle 64: Frage Q23 [F29] Schutzmaßnahmen

THEMA	Maßnahmen zum Schutz der persönlichen Daten im Internet allgemein
FILTER	ALLE
FRAGE	Welche der folgenden Maßnahmen haben Sie bereits ergriffen, um den Zugriff auf Ihre persönlichen Informationen im Internet zu kontrollieren? Bitte geben Sie alles Zutreffende an.
PROG	MEHRFACHANTWORT. ROTIEREN

Tabelle 65: Antwort Q23 [F29] Schutzmaßnahmen

Antwortmöglichkeiten	***Code***
Ich lese aufmerksam die Datenschutzerklärung, bevor ich meine personenbezogenen Daten im Internet weitergebe.	1
Ich habe die Zugriffsmöglichkeit auf meine geografischen Standortdaten (GPS) beschränkt.	2
Nur Personen, mit denen ich in sozialen Netzwerken verbunden bin, können die Inhalte meines Profils sehen.	3
Ich speichere keine persönlichen Daten (z. B. Kopien vom Führerschein, Personalausweis oder der Gesundheitskarte) in einem Online-Speicher (Cloud).	4
Ich verweigere regelmäßig meine Zustimmung, dass meine personenbezogenen Daten zu Werbezwecken verwendet werden.	5
Ich überprüfe regelmäßig den Sicherheitsstatus einer Website, auf der ich meine persönlichen Informationen angeben muss (z. B. Prüfung, ob es sich um eine https-Seite handelt, Sicherheitslogos/Zertifikate)	6
Ich habe Zugang zu den persönlichen Informationen beantragt, die Onlineplattformen über mich gespeichert haben, um diese Informationen aktualisieren oder löschen zu lassen.	7
Ich habe keine der genannten Maßnahmen durchgeführt (INT: NICHT VORLESEN) [PROG: EXKLUSIV, IMMER AN DIESER STELLE, Optisch von Item 1 bis 7 absetzen]	8

Demographie

Tabelle 66: D1 Demographie Schulbildung

THEMA	Schulbildung
FILTER	ALLE
FRAGE	Zum Abschluss haben wir noch einige Fragen zu Ihrer Person, die wir für die Statistik benötigen. Was ist Ihr höchster Schulabschluss?
PROG	-

Tabelle 67: Antwort D1 Demographie Schulbildung

Antwortmöglichkeiten	***Code***
Ohne Schulabschluss	1
Volks-/Hauptschulabschluss, Polytechnische Oberschule (POS) mit Abschluss 8. Klasse	2
Mittlere Reife / Realschulabschluss, Fachschulreife, Polytechnische Oberschule (POS) mit Abschluss 10. Klasse	3
Fachhochschulreife, Abschluss einer Fachoberschule oder Berufsausbildung mit Abitur	4
Abitur / Hochschulreife / Erweiterte Oberschule mit Abschluss 12. Klasse (EOS)	5
ein anderer Schulabschluss	6
noch Schüler, mit Abschlussziel Haupt-/Realschulabschluss	7
Noch Schüler, mit Abschlussziel Fach-/Hochschulreife	8
Keine Angabe	9

Tabelle 68: Frage D2 Demographie Berufsausbildung

THEMA	Berufsbildung
FILTER	ALLE
FRAGE	Und welches ist Ihr letzter Berufsbildungsabschluss:
PROG	-

Tabelle 69: Antwort D2 Demographie Berufsausbildung

Antwortmöglichkeiten	***Code***
Lehre/ Berufsausbildung im dualen System	1
Fachschulabschluss /Fachschulabschluss in der ehem. DDR	2
Bachelor	3
Master	4
Diplom	5
Promotion	6
in schulischer oder beruflicher Bildung	7
nicht in schulischer oder beruflicher Bildung	8
Keine Angabe	9

Tabelle 70: Frage D3 Demographie Berufstätigkeit

THEMA	Berufstätigkeit
FILTER	ALLE
FRAGE	Sind Sie derzeit...?
PROG	-

Tabelle 71: Antwort D3 Demographie Berufstätigkeit

Antwortmöglichkeiten	***Codes***
Ganztags berufstätig (mindestens 35 Stunden/Woche)	1
Teilzeit berufstätig (unter 35 Std./Woche, halbtags oder weniger)	2
Nicht berufstätig/Hausfrau/Hausmann	3
Erziehungsurlaub	4
zurzeit arbeitslos	5
in Rente/pensioniert	6
in Ausbildung/Studium/Wehr-/Zivildienst	7
Keine Angabe	9

Tabelle 72: Frage D4 Demographie Haushaltsgröße

THEMA	Haushaltsgröße
FILTER	ALLE
FRAGE	Kommen wir nun zu Ihrem Haushalt. Wie viele Personen leben ständig in Ihrem Haushalt, Sie selbst und Ihre Kinder mitgerechnet?
PROG	-

Tabelle 73: Antwort D4 Demographie Haushaltsgröße

Antwortmöglichkeiten	***Code***
___ Personen	-
Keine Angabe	99

Tabelle 74: Frage D5 Demographie Haushaltsangehörige

THEMA	Haushalt – Angehörige
FILTER	NUR WENN MEHR ALS 1 PERSON IN D4
FRAGE	Wer lebt außer Ihnen noch in Ihrem Haushalt?
PROG	MEHRFACHANTWORT

Tabelle 75: Antwort D5 Demographie Haushaltsangehörige

Antwortmöglichkeiten	***Code***
Ehe-/ Partner(in)	1
Kinder unter 6 Jahre	2
Kinder zwischen 6 und 13 Jahre	3
Kinder zwischen 14 und 15 Jahre	4
Kinder zwischen 16 und 17 Jahre	5
Kinder ab 18 Jahren	6
Andere Familienangehörige, z.B. Eltern oder Großeltern	7
Andere Personen, die nicht zur Familie gehören	8
Keine Angabe [PROG: EXKLUSIV]	9

Tabelle 76: Frage D6 (D5A2) Demographie Kinder unter 6 Jahren

THEMA	Haushalt – Kinder unter 6 Jahre
FILTER	NUR FÜR CODE 2 AUS D5
FRAGE	Sie sagten ja, dass Kinder unter 6 Jahre in Ihrem Haushalt leben. Wie viele Kinder sind das?
PROG	-

Tabelle 77: Antwort D6 (D5A2) Demographie Kinder unter 6 Jahren

Antwortmöglichkeiten	***Code***
___ Kinder unter 6 Jahre	-
Doch KEINE Kinder unter 6 Jahren im Haushalt	00
Keine Angabe	99

Tabelle 78: Frage D7 (D5A3) Demographie Kinder zwischen 6 und 13 Jahren

THEMA	Haushalt – Kinder zwischen 6 und 13 Jahre
FILTER	NUR FÜR CODE 3 AUS D5
FRAGE	Sie sagten ja, dass Kinder zwischen 6 und 13 Jahre in Ihrem Haushalt leben. Wie viele Kinder sind das?
PROG	-

Tabelle 79: Antwort D7 (D5A3) Demographie Kinder zwischen 6 und 13 Jahren

Antwortmöglichkeiten	***Code***
___ Kinder zwischen 6 und 13 Jahre	-
Doch KEINE Kinder zwischen 6 und 13 Jahre im Haushalt	00
Keine Angabe	99

Tabelle 80: Frage D8 (D5A4) Demographie Kinder zwischen 14 und 15 Jahren

THEMA	Haushalt – Kinder zwischen 14 und 15 Jahre
FILTER	NUR FÜR CODE 4 AUS D5
FRAGE	Sie sagten ja, dass Jugendliche zwischen 14 und 15 Jahre in Ihrem Haushalt leben. Wie viele Jugendliche sind das?
PROG	-

Tabelle 81: Antwort D8 (D5A4) Demographie Kinder zwischen 14 und 15 Jahren

Antwortmöglichkeiten	***Code***
___ Jugendliche zwischen 14 und 15 Jahre	-
Doch KEINE Jugendliche zwischen 14 und 15 Jahren im Haushalt	00
Keine Angabe	99

Tabelle 82: Frage D8a (D5A5) Demographie Kinder zwischen 16 und 17 Jahren

THEMA	Haushalt – Kinder zwischen 16 und 17 Jahre
FILTER	NUR FÜR CODE 5 AUS D5
FRAGE	Sie sagten ja, dass Jugendliche zwischen 16 und 17 Jahre in Ihrem Haushalt leben. Wie viele Jugendliche sind das?
PROG	-

Tabelle 83: Antwort D8a (D5A5) Demographie Kinder zwischen 16 und 17 Jahren

Antwortmöglichkeiten	***Code***
___ Jugendliche zwischen 16 und 17 Jahre	-
Doch KEINE Jugendliche zwischen 16 und 17 Jahren im Haushalt	00
Keine Angabe	99

Tabelle 84: Frage D8b (D5A6) Demographie Kinder ab 18 Jahren

THEMA	Haushalt – Kinder ab 18 Jahren
FILTER	NUR FÜR CODE 8 AUS D5
FRAGE	Sie sagten ja, dass Jugendliche 18 Jahre in Ihrem Haushalt leben. Wie viele Jugendliche sind das?
PROG	-

Tabelle 85: Antwort D8b (D5A6) Demographie Kinder ab 18 Jahren

Antwortmöglichkeiten	***Code***
___ Jugendliche ab 18 Jahre	-
Doch KEINE Jugendliche zwischen 16 und 17 Jahren im Haushalt	00
Keine Angabe	99

Tabelle 86: Frage D9 Demographie Einkommen

THEMA	Einkommen
FILTER	ALLE
FRAGE	CATI: Ich lese Ihnen jetzt sieben Einkommensgruppen vor. Zu welcher Gruppe gehört Ihr Haushalt? Gemeint ist das monatliche Netto-Einkommen aller Personen, die zu Ihrem Haushalts einkommen beitragen, nach Abzug von Steuern und Sozialabgaben. Vergessen Sie bitte nicht, eventuelle Zusatzzahlungen wie Wohn- oder Kindergeld hinzuzurechnen. Beträgt das monatliche Haushaltsnettoeinkommen Ihres Haushalts... CAWI: Sie sehen jetzt sieben Einkommensgruppen. Zu welcher Gruppe gehört Ihr Haushalt? Gemeint ist das monatliche Netto-Einkommen aller Personen, die zu Ihrem Haushaltseinkommen beitragen, nach Abzug von Steuern und Sozialabgaben. Vergessen Sie bitte nicht, eventuelle Zusatzzahlungen wie Wohn- oder Kindergeld hinzuzurechnen. Beträgt das monatliche Haushaltsnettoeinkommen Ihres Haushalts...
PROG	-

Tabelle 87: Antwort D9 Demographie Einkommen

Antwortmöglichkeiten	***Code***
Unter 750 Euro	1
750 bis unter 1500 Euro	2
1500 bis unter 2250 Euro	3
2250 bis unter 3000 Euro	4
3000 bis unter 4000 Euro	5
4000 bis unter 5000 Euro	6
5000 Euro und mehr	7
Weiß nicht (nicht vorlesen!)	8

Antwortmöglichkeiten	*Code*
Keine Angabe (nicht vorlesen!)	9

Tabelle 88: Frage D10 Demographie Postleitzahl

THEMA	Wohnort – Postleitzahl
FILTER	ALLE
FRAGE	Welche Postleitzahl hat Ihr Wohnort?
PROG	-

Tabelle 89: Antwort D10 Demographie Postleitzahl

Antwortmöglichkeiten	*Code*
___ PLZ	-
Keine Angabe	99999

Ergebnisse der Regressionsanalyse

Tabelle 90 Ergebnisse der Regressionsanalyse bzw. in das Modell aufgenommene Variablen

Variable	*ß*[21]	*t-Wert*[22]	*Signifikanz*	*Aussage*
Q5_1: Bedenken Onlineshopping: Dass die Ware nicht, falsch oder beschädigt bei mir ankommt	0,050	1,840	.	Je höher die Bedenken, dass die Ware nicht, falsch oder beschädigt ankommt, desto höher der Grad der Besorgtheit.
Q5_2: Bedenken Onlineshopping: Dass es sich nicht um einen tatsächlich existierenden Onlineshop handelt	0,071	2,514	*	Je höher die Bedenken, dass es sich nicht um einen tatsächlich existierenden Onlineshop handelt, desto höher der Grad der Besorgtheit.
Q5_3: Bedenken Onlineshopping: Dass meine persönlichen Daten weitergereicht werden	0,289	9,887	***	Je höher die Bedenken, dass die persönlichen Daten weitergereicht werden, desto höher der Grad der Besorgtheit.
Q11: Interesse für Themen rund um Datensicherheit beim Onlineshopping	0,025	0,998	n.s.	Kein Effekt des Interesses für Themen rund um Datensicherheit beim Onlineshopping auf den Grad der Besorgtheit.
Q12: Wahrscheinlichkeit, dass persönliche Daten beim Onlineshopping von Dritten unrechtmäßig eingesehen oder entwendet werden	0,232	9,072	***	Je höher die Wahrscheinlichkeit eingeschätzt wird, dass die persönlichen Daten beim Onlineshopping von Dritten unrechtmäßig eingesehen oder entwendet werden, desto höher der Grad der Besorgtheit.
Q13_2: Wahrgenommene Gefährlichkeit: Passwort zum E-	0,118	4,591	***	Je höher die wahrgenommene Gefährlichkeit, wenn das Passwort zum E-

[21] ß entspricht dem Regressionskoeffizient und zeigt den Einfluss bzw. Effekt der Variable in der Regressionsgleichung an.

[22] Testgröße des Hypothesentests

Variable	*ß*[21]	*t-Wert*[22]	*Signifikanz*	*Aussage*
Mailzugang wird gehackt.				Mailzugang gehackt wird, desto höher der Grad der Besorgtheit.
Q13_3: Wahrgenommene Gefährlichkeit: Meine Einkaufsliste wird weitergereicht.	0,149	5,546	***	Je höher die wahrgenommene Gefährlichkeit, wenn die Einkaufsliste weitergereicht wird, desto höher der Grad der Besorgtheit.
Q18_1: Wahrgenommene Informiertheit durch staatliche Institutionen	-0,025	-0,973	n.s.	Kein Effekt der wahrgenommenen Informiertheit durch staatliche Institutionen zum Thema auf den Grad der Besorgtheit
Q21_a: Informationsverhalten: Bereits zum Thema informiert in der Vergangenheit	0,044	1,732	.	Das Informationsverhalten in der Vergangenheit zum Thema hat einen signifikanten Effekt auf den Grad der Besorgtheit: Information in der Vergangenheit = ja hat einen positiven Effekt auf den Grad der Besorgtheit (=höhere Besorgtheit).
Q22_1: Selbstwirksamkeit: Wahrgenommene persönliche Beeinflussbarkeit der Datensicherheit	-0,047	-1,831	.	Je höher die wahrgenommene Selbstwirksamkeit, desto niedriger der Grad der Besorgtheit.
Q22_2: Ausgeliefertsein im Schadensfall	-0,025	-1,001	n.s.	Kein Effekt des wahrgenommenen Ausgeliefertseins im Schadensfall auf den Grad der Besorgtheit.
Q22_3: Erfahrungen mit Problemen bei Datensicherheit im Internet allgemein	0,093	3,764	***	Je mehr negative Erfahrungen mit Problemen bei Datensicherheit im Internet allgemein gemacht wurden, desto höher der Grad der Besorgtheit.

Variable	*ß*[21]	*t-Wert*[22]	*Signifikanz*	*Aussage*
Q22_4: Vorsichtigkeit in Bezug auf persönliche Daten	0,073	2,756	**	Je vorsichtiger im Internet in Bezug auf die persönlichen Daten ist, desto höher der Grad der Besorgtheit.

Signifikanzcodes: <0,001***; 0,001 **; 0,01 *; 0,1 .; n.s.=nicht signifikant

Nicht in das Modell aufgenommene Variablen

Tabelle 91 Nicht *mit in das Modell aufgenommene Variablen*

Nicht mit aufgenommener Variable	***Grund***
Q5_4: Bedenken Onlineshopping: Dass die persönlichen Daten unrechtmäßig eingesehen oder veröffentlicht werden	Hohe Korrelation mit Bedenken Onlineshopping: Dass meine persönlichen Daten weitergereicht werden.
Q5_5: Bedenken Onlineshopping: Dass mein Passwort für den Login zum Kundenbereich eines Onlineshops nicht sicher verschlüsselt wird	Hohe Korrelation mit Bedenken Onlineshopping: Dass meine persönlichen Daten weitergereicht werden.
Q13_1: Wahrgenommene Gefährlichkeit: Mein Gerät wird mit Schadsoftware infiziert, so dass ich es nicht mehr nutzen kann z. B. Virus, Trojaner.	Hohe Korrelation mit Bedenken Onlineshopping: Passwort zum Emailzugang wird gehackt.
Q13_4: Wahrgenommene Gefährlichkeit: Meine persönlichen Daten wie Name, Adresse etc. werden weitergereicht.	Hohe Korrelation mit Bedenken Onlineshopping: Einkaufsliste wird weitergereicht.
Q13_5: Wahrgenommene Gefährlichkeit: Meine Bank- bzw. Kreditkartendaten werden gestohlen.	Hohe Korrelation mit Bedenken Onlineshopping: Mein Passwort zum E-Mailzugang wird gehackt.
Q13_6: Wahrgenommene Gefährlichkeit: Auf meinem Gerät werden meine persönlichen Daten verschlüsselt, so dass ich diese nicht mehr nutzen kann.	Hohe Korrelation mit Bedenken Onlineshopping: Mein Passwort zum E-Mailzugang wird gehackt.
Q13_7: Wahrgenommene Gefährlichkeit: Meine Daten werden für Identitätsdiebstahl eingesetzt.	Hohe Korrelation mit Bedenken Onlineshopping: Mein Passwort zum E-Mailzugang wird gehackt.
Q18_2: Wahrnehmung Schutzgefühl durch staatliche Institutionen	Hohe Korrelation mit Wahrnehmung Informiertheit durch staatliche Institutionen.