Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Steuererklärungsapps

Änderungshistorie

Tabelle 1: Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
V1.0	20.02.2024	BSI WG 32	Initiale Berichterstellung

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

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Hintergrund der Studie

1.1 Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt für den aktiven Schutz der Menschen in der digitalen Welt eine entscheidende Rolle ein – als die zentrale Cybersicherheitsbehörde und unabhängige Stelle für den Digitalen Verbraucherschutz in Deutschland.

Hierfür untersucht das BSI im Rahmen der Marktbeobachtung regelmäßig einzelne Segmente des digitalen Verbrauchermarktes durch eine tiefergehende Analyse. Ziel ist es, auf Basis der gewonnenen Erkenntnisse Handlungsbedarfe zu identifizieren sowie eine Grundlage für die weitere Diskussion und Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft zu schaffen. Die Marktbeobachtung trägt damit zu einer ganzheitlichen Gestaltung eines wirksamen Digitalen Verbraucherschutzes in Deutschland und Europa bei.

Mit einem kooperativen Ansatz unserer Aktivitäten gemeinsam mit den Dienstanbietern steigern wir die IT-Sicherheit für konkrete Anwendungsfälle, Produkte bzw. Dienste im Verbraucheralltag. Unter anderem in Bezug auf identifizierte und geschlossene Schwachstellen in der IT-Sicherheit schützen wir damit die Menschen in der digitalen Welt aktiv vor den Gefahren der Digitalisierung und sorgen dafür, dass sie sich sicher online bewegen können.

Auch im Rahmen dieser technischen Untersuchung zu Steuererklärungsapps wirkte der kooperative Dialog mit den Dienstanbietern. Alle beteiligten Unternehmen haben offen und fachlich fundiert mit dem BSI zusammengearbeitet, sodass im Ergebnis die IT-Sicherheit im Bereich der Steuererklärungsapps spürbar vorangebracht werden konnte. Weitere Impulse setzen wir mit der Veröffentlichung dieses Abschlussberichts und mit der gezielten Adressierung der im Bereich dieses Untersuchungsscopes tätigen Wirtschaftsakteure.

Die Publikationsreihe „IT-Sicherheit auf dem digitalen Verbrauchermarkt“ bildet dabei die zentrale Veröffentlichung des BSI im Kontext der Beobachtung des digitalen Verbrauchermarktes und erscheint seit 2021 mit verschiedenen Schwerpunkten. Bisher sind in dieser Reihe folgende Publikationen erschienen:

- IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Onlineshopping-Plattformen
- IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Moderne Messenger
- IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheitsapps

Mit der vorliegenden Publikation wird die Reihe um die Produktkategorie der Steuererklärungsapps ergänzt.

1.2 Ausgangslage und Zielsetzung

Die fortschreitende Digitalisierung im Finanzsektor hat zu einer deutlichen Zunahme in der Nutzung von Steuererklärungsapps geführt. Dieser Trend wird durch eine repräsentative Umfrage des Digitalverbands Bitkom bestätigt, wonach bereits 57 % der Deutschen, die eine Steuererklärung abgeben, dies online tun. Dies unterstreicht die Bedeutung und das Wachstumspotenzial digitaler Lösungen in diesem Bereich. Besonders auffällig ist dabei die zunehmende Nutzung von Steuererklärungsapps auf Smartphones, die von vier Prozent im Jahr 2022 auf acht Prozent im Jahr 2023 gestiegen ist. Dies zeigt ein steigendes Interesse an mobilen Lösungen, die den Desktop als bevorzugtes Endgerät tendenziell ablösen könnten und führt zu einem verstärkten Trend hin zu App-basierten Lösungen.[1]

Diese Entwicklungen und die sensible Natur der Daten, die über diese Apps verarbeitet werden, unterstreicht die Notwendigkeit einer detaillierten technischen Untersuchung durch das BSI. Ziel ist es, ein

[1] Vgl. https://www.bitkom.org/Presse/Presseinformation/6-von-10-Steuererklaerungen-zuletzt-online-abgegeben

repräsentatives Bild über die IT-Sicherheit dieser Anwendungen zu gewinnen. Der Markt für Steuererklärungsapps, der durch sein Volumen und seine Wachstumsdynamik gekennzeichnet ist, wird zunehmend relevant. Mit der wachsenden Beliebtheit digitaler Lösungen wie der ELSTER[2]-Schnittstelle und Smartphone-Apps steigt auch die Nachfrage nach zuverlässigen und sicheren Anwendungen. Diese Marktdynamik bietet Chancen für Innovation, konfrontiert die Branche aber auch mit Herausforderungen, insbesondere in Bezug auf die Datensicherheit.

Die Untersuchung zielt darauf ab, Empfehlungen für die Weiterentwicklung und Verbesserung der IT-Sicherheit von Steuererklärungsapps zu geben. Besondere Aufmerksamkeit wird dabei der Anpassung an technologische Veränderungen gewidmet, um das Vertrauen der Nutzenden in digitale Lösungen zu stärken bzw. zu erhalten.

1.3 Aufbau und Methodik

Das BSI hat die vorliegende Studie erstellt und die Deutsche Telekom Security GmbH mit der technischen Analyse der Stichprobenapps beauftragt. Folgend wird der Ablauf der Studie dargestellt:

- Phase 1
  - Erstellung eines Marktüberblicks
  - Stichprobenauswahl
- Phase 2
  - Technische Untersuchung
  - Offenlegung der Prüfungsfeststellungen gegenüber Dienstanbietern
- Phase 3
  - Erstellung des Abschlussberichts

Im ersten Schritt erfolgte eine Analyse zu den auf dem deutschen Markt verfügbaren Steuererklärungsapps (weitere Details in Abschnitt 2.2). Die mit dieser Marktübersicht definierte Grundgesamtheit wurde über fachliche Auswahlkriterien eingeschränkt. Anschließend wurden über eine Zufallsstichprobe neun Apps für eine technische Untersuchung ausgewählt.

Zusätzlich wurde eine Recherche zu bereits bekannten Schwachstellen innerhalb der kompletten spezifischen Produktkategorie durchgeführt. Diese Recherche verlief jedoch hinsichtlich der jüngsten Vergangenheit ergebnislos, sodass hieraus keine Schwerpunktsetzung für den technischen Untersuchungsscope abgeleitet werden konnte.

Für jede technische Untersuchung erstellte die Deutsche Telekom Security GmbH einen Ergebnisbericht mit den identifizierten Schwachstellen und Sicherheitshinweisen in den getesteten Produkten. Diese Ergebnisberichte wurden durch das BSI den Dienstanbietern offengelegt und Stellungnahmen eingeholt.

Auf dieser Datenbasis wurde der vorliegende Abschlussbericht erstellt.

[2] Apronym für Elektronische Steuererklärung

2 Produkt und Markt

2.1 Beschreibung der Produktkategorie

Steuererklärungsapps sind eine digitale Lösung zur Vereinfachung des oft als komplex und zeitaufwendig empfundenen Prozesses der Erstellung einer Steuererklärung. Technisch gesehen sind die meisten dieser Apps plattformübergreifend verfügbar, sowohl für iOS- als auch für Android-Geräte. Einige Dienstanbieter haben zusätzlich oder ausschließlich Web-Versionen im Portfolio.

Das Hauptmerkmal der Steuererklärungsapps ist ihre Benutzerfreundlichkeit im Sinne einer in der Regel über ein Fragen-Antwort-System geführten Befüllung der Formblätter. Dabei wird überwiegend die Erstellung von Einkommenssteuererklärungen in einfachen Anwendungsfällen fokussiert.

Weiterhin bieten diese Apps in der Regel an, dass Steuerdaten aus den Vorjahren direkt übernommen und lediglich auf Aktualität geprüft werden müssen. Hierdurch soll der Arbeitsaufwand für Nutzende minimiert werden, es entsteht gleichzeitig aber auch ein Lock-in-Effekt, der sich auf die Wechselbereitschaft der Nutzenden auswirkt.

Je nach Dienstanbieter sind auch automatisierte Funktionen wie der Import von Lohnsteuerbescheinigungen und anderen relevanten Dokumenten und Belegen verfügbar.

Neben der Kernfunktionalität Erstellung einer Steuererklärung durch die Nutzenden selbst, bieten viele dieser Apps zusätzliche Dienstleistungen, wie zum Beispiel den direkten Kontakt zu Steuerberaterinnen und -beratern oder die Möglichkeit, die Erklärung direkt aus der App an das Finanzamt zu übermitteln.

Für diese technische Untersuchung wird die Produktkategorie der Steuererklärungsapps von klassischer Steuererklärungssoftware für den Heim-PC abgegrenzt. Letztere wird in der Regel auf einem Desktop- oder Laptop-Computer installiert. Sie ist oft für Windows oder macOS optimiert und benötigt in der Regel eine stabile Internetverbindung für Updates oder zum Abrufen bestimmter Informationen, aber nicht zwangsläufig für die gesamte Nutzungsdauer. Hintergrund ist, dass Daten in der Regel auf dem lokalen Computer gespeichert und verarbeitet werden. Steuererklärungsapps hingegen sind für mobile Geräte wie Smartphones und Tablets konzipiert. Diese Apps erfordern in der Regel eine ständige Internetverbindung, da die Datenverarbeitung und -speicherung überwiegend im Backend, also auf den Servern des Dienstanbieters erfolgt.

2.2 Marktanalyse

Die Marktanalyse konkretisiert die Beschreibung der Produktkategorie aus dem vorhergehenden Abschnitt 2.1 und ist ein wesentliches Fundament für die Berücksichtigung des Neutralitätsgebots. Es handelt sich hierbei um ein grundsätzliches Prinzip, das bei sämtlichen administrativen und operativen Entscheidungen der Bundesverwaltung, einschließlich der Strichprobenauswahl für technische Untersuchungen, strikt beachtet werden muss. In Bezug auf die Überprüfung von Steuererklärungsapps bedeutet das, diese Auswahl frei von jeglichen Vorurteilen, Bevorzugungen und Benachteiligungen von einzelnen Produkten oder Diensten zu treffen.

Die Auswahl sollte eine repräsentative Mischung verschiedener Steuererklärungsapps abdecken, um ein umfassendes und ausgewogenes Bild zu gewährleisten. Dies kann durch den Einsatz von zufälligen Auswahlmethoden oder durch die Definition spezifischer, objektiver Kriterien erreicht werden, die auf die Gesamtheit der verfügbaren Steuererklärungsapps angewendet werden.

Die Einhaltung des Neutralitätsgebots gewährleistet, dass die Ergebnisse der technischen Untersuchung glaubwürdig sind und das Vertrauen der Öffentlichkeit in die Bundesverwaltung gestärkt wird. Dadurch wird sichergestellt, dass alle Dienstanbieter gleichbehandelt werden und dass die Ergebnisse der Untersuchung allein auf den technischen Merkmalen und Leistungen der Apps basieren, frei von jeglicher Beeinflussung durch externe Faktoren.

In diesem Kapitel wird die Eingrenzung des relevanten Marktes transparent dargestellt.

Kriterium 1: Anbindung an die ELSTER-Schnittstelle, Erfüllung der Anforderungen des § 87c AO
Die ELSTER-Schnittstelle spielt eine zentrale Rolle bei der digitalen Abgabe von Einkommenssteuererklärungen in Deutschland. ELSTER, kurz für „Elektronische Steuererklärung", ist eine Initiative der deutschen Steuerverwaltung, die darauf abzielt, Steuererklärungsprozesse zu digitalisieren und zu vereinfachen. Hierdurch wird es ermöglicht, die Steuerdaten digital zu erfassen, an das Finanzamt zu übertragen und je nach Wunsch der steuerpflichtigen Person, auch die weitere Kommunikation und Bereitstellung des Steuerbescheids digital abzubilden. ELSTER bietet sowohl für Steuerpflichtige als auch für die Finanzverwaltung erhebliche Vorteile in Bezug auf Effizienz, Genauigkeit und Benutzerfreundlichkeit. Aus diesen Gründen werden in dieser technischen Untersuchung nur Steuererklärungsapps betrachtet, die eine entsprechende Datenübertragung via ELSTER an die Finanzverwaltung für ihre Nutzenden zur Verfügung stellen. Ausgeschlossen sind damit beispielsweise Apps, die Nutzende zwar bei der Befüllung der Einkommenssteuererklärung unterstützen, diesen aber die Übertragung an das Finanzamt (beispielsweise durch ausgedruckte und gezeichnete Formulare) komplett selbst überlassen. Diese Selektierung in der Produktauswahl wird zudem getroffen, da seitens des BSI angenommen wird, dass durch die Ende-zu-Ende-Digitalisierung bei Nutzung der ELSTER-Schnittstelle ein höherer Mehrwert geschaffen wird und sich diese Produkte daher langfristig am Markt etablieren können.

Im ELSTER-Onlineportal ist eine Auflistung von Softwareprodukten veröffentlicht, die eine Anbindung an die ELSTER-Schnittstelle anbieten und damit bereits Kriterium 1 erfüllen. Es ist seitens des BSI davon auszugehen, dass alle Dienstanbieter, welche die gesetzlichen Anforderungen zur Nutzung der ELSTER-Schnittstelle erfüllen und öffentlich genannt werden wollen, in dieser Liste aufgeführt sind. Hierfür müssen die Anbieter gesetzliche Anforderungen erfüllen, welche die Finanzbehörden überprüfen können (vgl. § 87c AO). Es kann davon ausgegangen werden, dass die Produkte, welche die gesetzlichen Anforderungen nach § 87c AO erfüllen und sich ggf. überprüfen lassen müssen, auch im ELSTER-Onlineportal listen lassen. Denn um ihren Dienst anbieten zu können, müssen sie entsprechenden regulatorischen Aufwand in Kauf nehmen, erhalten durch die Listung im Portal aber Sichtbarkeit bei der Zielgruppe.

Kriterium 2: Mobile Apps im engeren Sinne
Die technische Untersuchung fokussiert auf Software, die für mobile Anwendungen wie Tablets und Smartphones ausgelegt ist. Hintergrund dieser Schwerpunktsetzung ist der eingangs erwähnte Trend zur Abgabe der Steuererklärung via mobiler Geräte und Endanwendungen. Hiermit ist nach aktuellem Kenntnisstand die laufende Übertragung der Daten an Backendsysteme verbunden. Software, welche für die Installation auf Desktop-PCs, Notebooks o.ä. vorgesehen ist, verarbeitet die Daten und erstellt die Steuererklärung in der Regel auf dem Client selbst, besitzt damit ein abweichendes Risikoprofil und wird in der Marktanalyse ausgeschlossen.

Kriterium 3: Einkommenssteuererklärung
Das BSI fokussiert die vorliegende technische Untersuchung auf den Digitalen Verbraucherschutz. Die häufigste Form der Steuererklärung aus der Zielgruppe der Verbraucherinnen und Verbraucher ist die Einkommenssteuererklärung. Somit werden ausschließlich Apps betrachtet, welche diese Art der Steuererklärung unterstützen.

Gemäß Datenabruf im ELSTER-Onlineportal vom 29.09.2021 wurden die Kriterien 1 und 3 von 70 Softwareprodukten erfüllt. Das Kriterium 2 wurde durch eine individuelle Prüfung der vorausgewählten Produkte angewendet.

Weiterhin wurden folgende Datenbereinigungen vorgenommen:

- Die Filterung auf Einkommenssteuererklärungen ist zielgruppenunspezifisch, sodass das Kriterium 3 ungenügend in der Vorfilterung abgebildet war. Softwareprodukte, die sich explizit an Steuerberaterinnen und –berater richten, wurden manuell aus der Auswahl entfernt.

- Die Überprüfung von Webseiten und App Stores zeigte in einigen Fällen, dass die Dienste nicht mehr angeboten werden. Auch diese wurden aus der Auswahl entfernt.
- Einige Unternehmen vermarkten ihren Dienst zielgruppenspezifisch. Technisch wird jedoch die gleiche Basis genutzt. Auch diese Redundanzen wurden bereinigt.
- Sollten Unternehmen mehrere Produkte im Einsatz haben, welche die bisherigen Kriterien und Bereinigungen durchlaufen haben, so wurde lediglich das nach BSI-Einschätzung identifizierte Hauptprodukt übernommen.

3 Vorbereitung der technischen Untersuchung

3.1 Produktauswahl

Die Produktauswahl erfolgte per Zufallsauswahl auf Basis der vorgelagerten Marktanalyse aus Abschnitt 2.2 dieses Berichts. Es wurden neun Steuererklärungsapps ausgewählt, hierunter drei Web-Apps, vier Android-Apps und zwei iOS-Apps.

3.2 Prüfungsvorgehen

Apps für mobile Endgeräte funktionieren in einem komplexen technischen Zusammenspiel zwischen der eigentlichen Anwendung, dem Smartphone, dem Betriebssystem und den externen Kommunikationsmöglichkeiten des Gerätes. Diese Ausgangssituation erlaubt sehr unterschiedliche Prüftiefen. Im vorliegenden Fall erfolgte die technische Untersuchung als Black-Box-Analyse auf Basis eines zwischen BSI und Penetrationstestern abgestimmten, internen Durchführungskatalogs. Die Testdurchführung erfolgte dabei durch die im Folgenden genannten Schritte:

- Automatisierte Analyse (statisch) der App-Installationsdatei
- Automatisierte Analyse der App
- Live-Analyse in definierter Testumgebung
- Manuelle Prüfung der App (inkl. Verifikation von potentiellen Schwachstellen aus Schritt 1 und 2)
- Prüfung der Kommunikations-Endpunkte der Backend-Systeme
- Erstellung des Prüfberichts

Der Umfang der einzelnen Schwachstellenanalysen erfolgte fokussiert, sodass für die erweiterte Prüfung verschiedene, ausgewählte sicherheitsrelevante Funktionen der Apps untersucht wurden:

- Allgemeine Schutzmaßnahmen der Anwendung
- Speicherung von Nutzerdaten und Datensparsamkeit
- Registrierung, Authentifizierung und Session Management

Folgende, im Digitalen Verbraucherschutz relevante Aspekte waren in dieser technischen Untersuchung nicht im Scope:

- Bereitstellung und Informationstransparenz bzgl. Updates
- Usable Security
- Incident Response und Recovery
- Accountwiederherstellungsprozess
- Tiefergehende Analysen von z. B. Speichermedien
- Code Audits mit Reverse Engineering Techniken

Aufgrund des begrenzten Zeitansatzes achteten die Penetrationstester bei der Durchführung nicht darauf, von den Detektionssystemen der Dienstanbieter unentdeckt zu bleiben. Teilweise wurden diese Systeme durch die Dienstanbieter für Zwecke des Testes auch abgeschaltet bzw. wurden Warnmeldungen nach Rücksprache mit dem Prüfteam missachtet.

Wie eingangs erwähnt, beschränkt sich die technische Untersuchung auf die Analyse der Binärdatei, also der kompilierten und ausführbaren Version des Programms, ohne Zugriff auf den zugrundeliegenden Quellcode zu haben. Die Penetrationstester kannten daher die internen Mechanismen der Apps nicht.

Stattdessen untersuchten sie, wie das Programm während der Ausführung auf verschiedene Eingaben und Interaktionen von außen reagiert.

Diese Methode wird oft bei Sicherheitsaudits, Penetrationstests oder Funktionsprüfungen eingesetzt, besonders wenn der Quellcode aus verschiedenen Gründen nicht verfügbar ist. Obwohl eine Black-Box-Analyse wertvolle Einblicke in die Sicherheit und Funktionalität eines Programms liefern kann, hat sie ihre Grenzen, da sie keine vollständige Sicht auf mögliche Sicherheitslücken oder Fehler im Code bietet, die nur durch eine Untersuchung des Quellcodes selbst identifiziert werden könnten. Im vorliegenden Fall wurde jedoch das Ziel verfolgt, den sicherheitstechnischen Gesamtzustand der betrachteten Steuererklärungsapps anhand einer Stichprobe zu erfassen, um Rückschlüsse auf die allgemeine Lage am Markt ziehen zu können. Hierfür kann eine Black-Box-Analyse als hinreichend angesehen werden.

3.3 Schwachstellenbewertung

Zur Ermittlung des Risikograds von Schwachstellen kam das Common Vulnerability Scoring-System (CVSS) in Version 3.1 zum Einsatz.[3]

Für jede gefundene Schwachstelle berechneten die Penetrationstester den CVSS Base Score und nahmen diesen Wert als Kritikalitätsbewertung der Schwachstelle in den Bericht zu den Prüfungsfeststellungen 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 („low“) 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, werden anhand der drei Kernschutzziele der Informationssicherheit 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

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

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 der Variable Scope, welcher die Auswirkungen eines Angriffs beschreibt. Hierbei kann der Wert „unchanged“ gewählt werden, wenn die Schwachstelle lediglich Auswirkungen besitzt, die sich auf die Komponente selbst beziehen. Der Wert „changed“ wird gewählt, falls noch weitere Komponenten existieren, auf die eine Ausnutzung der Schwachstelle Auswirkungen hat.

Die Penetrationstester bewerteten jede Schwachstelle anhand der skizzierten Metriken, so dass sich auf Basis einer vorgegebenen Formel, der Base Score auf einer Skala von 0 bis 10 ergab. In der folgenden Tabelle ist die Zuweisung des ermittelten Wertes zu einem Risikograd abgebildet:

Tabelle 2: CVSS Base Score und zugeordneter Risikograd

Risikograd	**Base Score**
Info	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Prüfungsfeststellungen mit dem Risikograd „Info“ haben einen informellen Charakter, markieren aber trotzdem ein Verbesserungspotential für die Systemsicherheit. Diese Kategorie kann ebenfalls für eine Beschreibung von nicht sicherheitsrelevanten Fehlern verwendet werden.

Es ist zu berücksichtigen, dass der Base Score üblicherweise auf Basis einer allgemeinen Bewertung des Sachverhalts ermittelt wird. Die Assets des betroffenen Systems oder der Komponente werden hierbei nicht berücksichtigt. Hierzu dient die Offenlegung gegenüber den Dienstanbieter nach Abschluss der technischen Untersuchung sowie deren Stellungnahme (vgl. hierzu Abschnitt 4.3).

4 Ergebnisse der technischen Untersuchung

4.1 Statistische Auswertung

In allen neun Apps der Stichprobe konnten die Penetrationstester Schwachstellen identifizieren. Bei der Verteilung der Prüfungsfeststellungen sticht eine App positiv heraus, die lediglich zwei Feststellungen mit dem Risikograd „medium“ und „low“ sowie eine „Info“-Feststellung verzeichnet (vgl. Abbildung 1). Bei allen anderen Apps können aus der rein quantitativen Betrachtung keine Auffälligkeiten abgeleitet werden, wenngleich beispielsweise bei „App 7“ über 20 Prüfungsfeststellungen zu verzeichnen sind. Hiervon entfallen jedoch elf Stück auf den Risikograd „Info“ und besitzen lediglich einen informellen Charakter (vgl. Abschnitt 3.3).

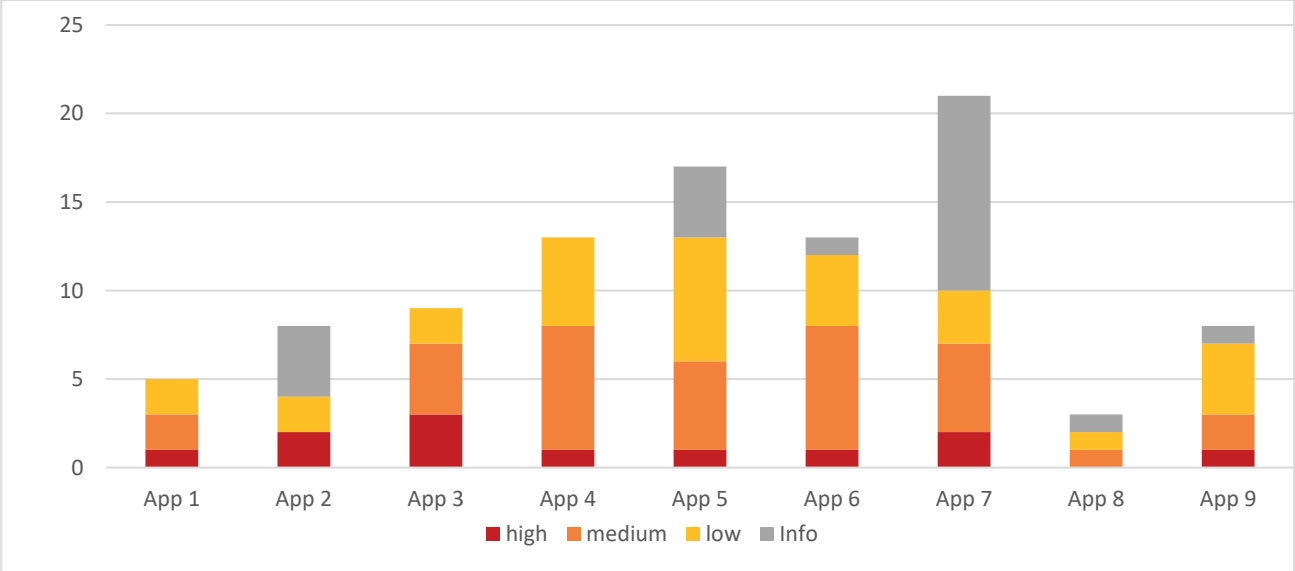

Abbildung 1: Verteilung der Prüfungsfeststellungen je App und Risikograd

Insgesamt konnten die Penetrationstester über alle neun Apps der Stichprobe hinweg 97 Prüfungsfeststellungen aller Risikograde identifizieren. Diese wurden für die weitere Auswertung fachlich qualifiziert thematisch zusammengefasst. Die Cluster mit den häufigsten Feststellungen können der Abbildung 2 entnommen werden.

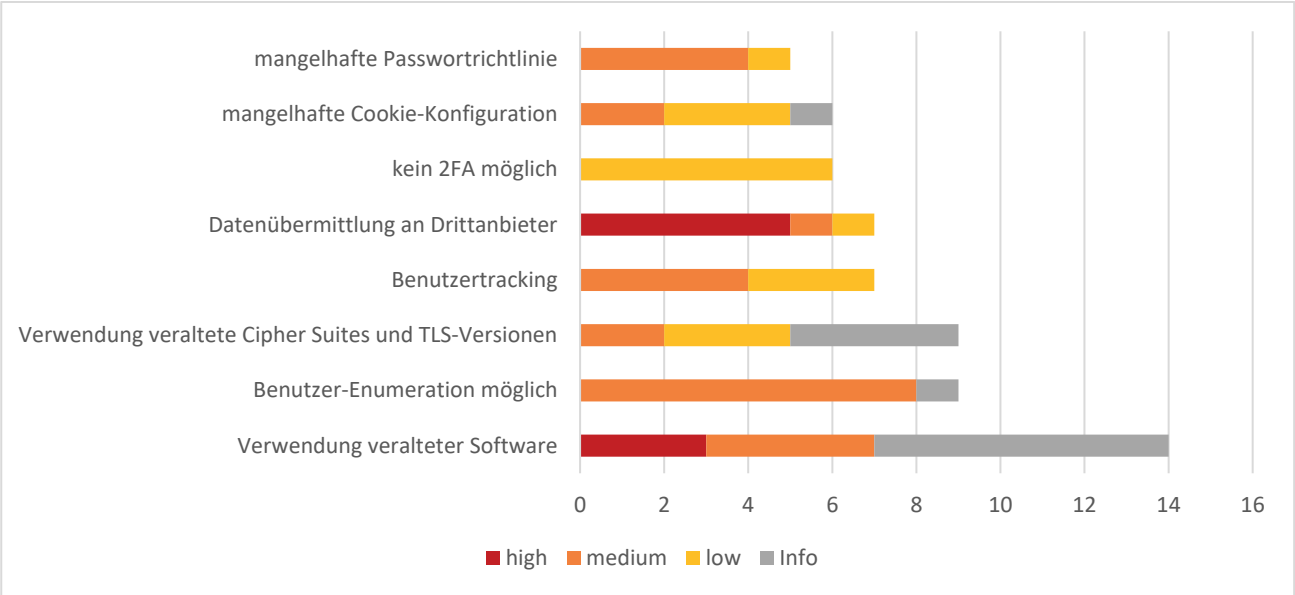

Abbildung 2: Feststellungscluster mit einem Anteil von mindestens fünf Prozent an den Gesamtfeststellungen

Die Feststellungen mit dem höchsten Risikograd „high“ verteilen sich wie folgt auf die Cluster:

- Datenübermittlung an Drittanbieter (5)
- Verwendung veralteter Software mit bekannten Schwachstellen (3)
- Risiko einer XSS-Injektion (2)
- Session-Fixation-Schwachstelle (1)
- Web-View-Inhalte austauschbar (1)

Weitere Prüfungsfeststellungen wurden in folgenden Clustern getroffen:

- Mangelhafte Konfiguration des http-Security-Header
- Fehler im Logout-Prozess
- Verwendete Software(komponenten) sind end of life
- Information Disclosure
- Unsichere Identifizierung möglich
- Unsichere http-Verbindung
- Nicht zweckmäßige Berechtigungsanfrage
- CORS-Fehlkonfiguration
- Fehlende Legitimation vor Datenänderung
- Unvollständige Datenlöschung
- Fehlende Datenmaskierung
- Open Redirect
- Schwacher Passwort-Hash
- Potentieller Passwort-Leak
- Test/Debug-Funktion aktiviert
- Ticket-Nummer Bypass
- Mangelhafte Zertifikatskonfiguration

Im folgenden Abschnitt wird näher auf eine Auswahl der Prüfungsfeststellungen eingegangen.

4.2 Darstellung der Prüfungsfeststellungen

4.2.1 Prüfungsfeststellungen mit Risikograd „high“

4.2.1.1 Datenübermittlung an Drittanbieter

Die Penetrationstester trafen 7 Prüfungsfeststellung zu potentiellen Datenübermittlungen an Drittanbieter. Hiervon wurden fünf Fälle mit Risikograd „high“ eingestuft.

In einem dieser fünf Fälle wurde festgestellt, dass personenbezogene Daten, unter anderem alle eingegebenen Steuerdaten an das Produkt „Sentry“ des Anbieters „Functional Software Inc.“ gesendet wurden. Es wurde erkannt, dass die Übertragung von personenbezogenen Daten unregelmäßig auftritt, wobei dies zumindest im Falle von Fehlern geschieht. Ebenso konnte erkannt werden, dass Authentifizierungsdaten an Sentry übertragen wurden. In diesen Fällen kann nicht ausgeschlossen werden, dass die übermittelten personenbezogenen Daten durch den Anbieter von „Sentry“ eingesehen werden

können. Die Datenschutzerklärung deckt dieses Datentransferverhalten nicht ab. Hier wird lediglich auf eine anonyme Erhebung und die Nutzung der Daten ohne Personenbezug verwiesen.

Die weiteren vier Prüfungsfeststellungen beziehen sich auf die Nutzung von Cloudflare. Es muss davon ausgegangen werden, dass dieser Dienstleister jederzeit die transportverschlüsselten Anfragen und Antworten zwischen der App und dem Backend einsehen kann, da dieser gleichzeitig auch Herausgeber des notwendigen SSL-Zertifikats ist. Nutzerinnen und Nutzer der Steuererklärungsapps müssen davon ausgehen, dass übermittelte personenbezogenen Daten, wie z.B. die Steuerdaten, von Cloudflare eingesehen werden können. Dieser Sachverhalt geht für Nutzerinnen und Nutzer nicht aus den Datenschutzerklärungen hervor und sollte aus Sicht des BSI explizit aufgeführt werden.

Weiterhin konnten die Prüfer zum Zeitpunkt der technischen Untersuchungen IP-Adressen von Cloudflare aus den Vereinigten Staaten von Amerika im DNS-Eintrag für die geprüften (Sub-) Domains identifizieren. Hierzu muss aber einschränkend erwähnt werden, dass Cloudflare-Rechenzentren unabhängig vom Standort den gleichen IP-Adressbereich annoncieren können. Auf Basis der IP-Adresse kann also nicht verlässlich identifiziert werden, in welches Zielland die Datenübermittlung erfolgt.

Das Hinzuziehen von Dienstleistern zum Schutz vor Distributed Denial of Service (DDoS)-Angriffen ist grundsätzlich begrüßenswert. Auch kann in bestimmten Fällen eine zuverlässige Mitigation nur durch das Aufbrechen eines TLS-verschlüsselten Datenstroms erfolgen. Es obliegt letztlich dem Betreiber hierfür einen Dienst auszuwählen der vertrauenswürdig und DSGVO-konform ist, sofern personenbezogene Daten betroffen sein könnten. Die notwendige Interessens- und Risikoabwägung muss dabei auf Basis der technisch notwendigen, nicht der technisch möglichen Maßnahmen erfolgen. Eine abschließende, immer für den konkreten Fall zu treffende Bewertung obliegt jedoch nicht dem BSI, sondern fällt in die Zuständigkeit der Datenschutzaufsichtsbehörden.

4.2.1.2 Verwendung veralteter Software mit bekannten Schwachstellen

Die Verwendung veralteter Software in Apps führt regelmäßig zu gravierenden IT-Sicherheitsrisiken. Eines der Hauptprobleme ist das Vorhandensein bekannter Schwachstellen in älterer Software. Diese Lücken sind oft in öffentlichen Datenbanken dokumentiert und bieten Angreifern leicht zugängliche Angriffspunkte. Ohne regelmäßige Updates fehlt es an wichtigen Sicherheitspatches, die gleichsam neue Schwachstellen adressieren. Dadurch steigt die Anfälligkeit der Apps für Cyberangriffe.

Zudem kann veraltete Software inkompatibel zu modernen Sicherheitsprotokollen und -standards sein, was die Sicherheit und Vertraulichkeit von Nutzerdaten zusätzlich gefährdet. Dies erhöht das Risiko von Sicherheitsverletzungen, die zu Datenlecks, Systemkompromittierungen und anderen schwerwiegenden Sicherheitsvorfällen führen können.

Daher ist es von entscheidender Bedeutung, dass Dienstanbieter ihre Software regelmäßig auf den neuesten Stand bringen. Dies umfasst nicht nur die Hauptanwendung, sondern auch alle eingebetteten Bibliotheken und genutzten Frameworks. Regelmäßige Updates sind unerlässlich, um die Sicherheit der Apps zu gewährleisten und den Schutz der Benutzerdaten zu garantieren.

Insgesamt trafen die Penetrationstester 14 Prüfungsfeststellungen hinsichtlich der Verwendung von veralteter Software. Diese verteilen sich auf die Risikograde „high“, „medium“ und „Info“. Im Folgenden wird auf die drei Feststellungen mit Risikograd „high“ eingegangen:

- Die eingesetzte Version des Apache Webservers ist von einer HTTP-Request Smuggling Schwachstelle betroffen (CVE-2022-22720). Bei fehlerhaften Anfragen scheitert der Webserver daran, die eingehende Verbindung zu schließen, wodurch weitere Anfragen eingeschleust werden können. Request Smuggling ist eine schwerwiegende Sicherheitsbedrohung, die Webserver erheblich gefährden kann. Diese Angriffstechnik kann dazu führen, dass Angreifer die Schwachstellen in der Verarbeitung von HTTP-Anfragen ausnutzen, um Benutzerdaten zu stehlen, bösartige Aktionen auszuführen oder sogar den gesamten Webserver zu kompromittieren. Die Auswirkungen von Request Smuggling können vielfältig sein, von der Beeinträchtigung der Verfügbarkeit von Webdiensten bis hin zur unbefugten

Manipulation von Inhalten und Sessions. Darüber hinaus kann Request Smuggling auch dazu verwendet werden, andere Schwachstellen im System auszunutzen, was zu weitreichenden Sicherheitsverletzungen führen kann.

- Die eingesetzte Version des Apache Tomcat Webservers ist möglicherweise anfällig für mehrere Denial of Service (DoS) Angriffe: CVE-2021-30639, CVE-2021-42340, CVE-2023-44487.
  Die Schwachstellen wurde jedoch aufgrund des möglichen Ausfalls des Systems nicht verifiziert. DoS-Angriffe zielen auf die Verfügbarkeit der Systeme ab. Oft ist die Anwendung nicht mehr verfügbar, bis diese neugestartet wurde.
- Die verwendete Version von Grafana ist veraltet und möglicherweise von folgenden Schwachstellen betroffen: CVE-2022-23498: Übernahme von Benutzersessions (CVSS „high“), CVE-2022-23552: Persistentes Cross-Site-Scripting (XSS) (CVSS „high“), CVE-2023-0507: Persistentes XSS (CVSS „high“), CVE-2023-0594: Persistentes XSS (CVSS „high“), CVE-2023-1387: Möglicher Leak des JWT als URL-Query Parameter (CVSS „medium“), CVE-2023-1410: Persistentes XSS (CVSS „medium“).

Diese Prüfungsfeststellungen gehen in der Regel mit der Problematik des Information Disclosures einher, also der Offenlegung sensibler Informationen. Ein besonders kritisches Beispiel hierfür ist die Offenlegung von Versionsangaben der eingesetzten Software. Wenn eine App oder ein System Informationen über ihre verwendeten Softwareversionen preisgibt, kann dies für potentielle Angreifer wertvolle Hinweise liefern. Insbesondere wenn es sich um veraltete oder nicht mehr unterstützte Versionen handelt, ermöglicht es Angreifern, gezielt nach bekannten Schwachstellen zu suchen. Diese Informationen können beispielsweise durch Fehlermeldungen, in den Metadaten von Webseiten oder sogar in den App-Einstellungen offengelegt werden. Ein Angreifer kann auf dieser Basis zielgerichtete Angriffe entwickeln, die auf bekannte Sicherheitslücken in dieser Version abzielen. Die Offenlegung von Versionsinformationen in Kombination mit fehlenden Sicherheitsupdates schafft ein perfektes Umfeld für Cyberangriffe.

4.2.1.3 Risiko einer XSS-Injection

In zwei Fällen stellten die Prüfer eine Anfälligkeit für Reflected Cross-Site Scripting (XSS) fest. XSS ist eine Angriffsart, bei dem Angreifer bösartigen Code in eine Webanwendung einschleusen, der dann an unwissende Nutzende weitergegeben wird. Dies geschieht typischerweise, indem der Angreifer eine Benutzerin bzw. einen Benutzer dazu verleitet, eine präparierte URL zu öffnen, die den schädlichen Skriptcode enthält. Wenn die Person die URL öffnet, wird der Code vom Webbrowser interpretiert und ausgeführt, als ob er von der vertrauenswürdigen Webseite stamme.

Die Ursachen für solche XSS-Angriffe liegen häufig in unzureichenden Eingabevalidierungs- und -sanitarisierungsmaßnahmen der Apps. Viele Webanwendungen akzeptieren Benutzereingaben, wie z.B. Suchanfragen oder Formulardaten, ohne diese angemessen zu prüfen oder zu bereinigen. Wenn diese Eingaben direkt in die generierte HTML-Seite eingebettet werden, ohne jegliche Überprüfung oder Bereinigung, können Angreifer schädlichen JavaScript-Code einschleusen.

Das Risiko eines solchen Angriffs ist beträchtlich, da es die Integrität und Vertraulichkeit der Benutzerdaten gefährdet. Durch den ausgeführten Skriptcode können Angreifer auf sensible Informationen wie Sitzungscookies und persönliche Daten zugreifen, was zu Identitätsdiebstahl, Betrug oder anderen Formen von Cyberkriminalität führen kann. Darüber hinaus kann ein erfolgreich durchgeführter XSS-Angriff das Vertrauen in die betroffene App untergraben und zu einem Reputationsverlust für das Entwicklungsteam oder das Unternehmen führen.

4.2.1.4 Session-Fixation-Schwachstelle

Eine Prüfungsfeststellung wurde hinsichtlich einer Session Fixation-Schwachstelle getroffen. Hierbei handelt es sich um eine IT-Sicherheitsschwachstelle, die bei Webanwendungen auftritt und bei der ein Angreifer eine gültige Session-ID einem Opfer aufzwingt, bevor dieses sich authentifiziert. Eine verbreitete Methode der Session Fixation involviert den Einsatz eines speziellen Session-Identifikators, wie beispielsweise eines sfsessid Parameters in einer URL oder eines Cookies.

Bei dieser Angriffsmethode generiert der Angreifer zuerst eine gültige Session-ID durch einen normalen Zugriff auf die betreffende Webanwendung. Anschließend trickst der Angreifer das Opfer mittels Phishing oder anderen Taktiken aus, eine URL mit dieser vorgegebenen Session-ID zu besuchen. Sobald das Opfer über die manipulierte URL auf die Webanwendung zugreift und sich authentifiziert, wird die Session, die ursprünglich vom Angreifer erstellt wurde, für das Opfer übernommen. Da die Session-ID bereits vor der Authentifizierung des Opfers festgelegt wurde, kann der Angreifer Zugang zur Session und somit potentiell zu sensiblen Daten oder Funktionen innerhalb der Anwendung erlangen.

Das Risiko dieser Schwachstelle liegt in der Möglichkeit, dass Angreifer unbefugten Zugriff auf Benutzerkonten erlangen können, ohne deren Anmeldedaten zu kennen. Dies stellt eine ernsthafte Bedrohung für die Sicherheit und Privatsphäre der Nutzerinnen und Nutzer dar und kann zu Datenlecks, Identitätsdiebstahl und anderen Formen von Cyberangriffen führen.

4.2.1.5 Web-View-Inhalte austauschbar

In einem Fall bestand die Funktionalität der App ausschließlich darin, die mobile Webseite innerhalb einer Web-View darzustellen. Aufgrund der Implementierung zur Darstellung der Webseite ließ sich dies in derartiger Form ausnutzen, dass die App mit beliebigen Inhalten gestartet werden konnte.

Durch eine von einem Angreifer durchgeführte Manipulation ist für Nutzerinnen und Nutzer nur erschwert erkennbar, dass sie sich nicht auf der Webseite bewegen, die durch die Verwendung der App besucht werden sollte. Im schlimmsten Fall können dadurch hoch sensible Daten an einen Angreifer gelangen.

4.2.2 Prüfungsfeststellungen mit häufigen Auftreten

4.2.2.1 Verwendung veraltete Software

Dieser Sachverhalt umfasst 14 % aller Prüfungsfeststellungen. Weitere Details können dem Abschnitt 4.2.1.2 entnommen werden.

4.2.2.2 Benutzerenumeration möglich

9 Prozent der Prüfungsfeststellungen beziehen sich auf das Risiko einer Benutzerenumeration. Hierbei wird es Angreifern ermöglicht, gültige Benutzernamen oder E-Mail-Adressen in einem System zu identifizieren. Dieses Risiko entsteht oft durch inkonsistente oder zu informative Rückmeldungen von Apps während des Authentifizierungsprozesses. Beispielsweise kann eine App unterschiedliche Fehlermeldungen anzeigen, je nachdem, ob der eingegebene Benutzername existiert oder nicht, oder ob das Passwort falsch ist. Solche Unterschiede bieten Angreifern Anhaltspunkte, um gültige Konten zu identifizieren.

Das Risiko von Benutzerenumeration liegt in mehreren Aspekten. Erstens ermöglicht es Angreifern, eine Liste von gültigen Benutzerkonten zu erstellen, was ein initialer Schritt für weitere Angriffe mittels Brute Force oder Phishing sein kann. Zweitens kann es zu einem Verlust des Vertrauens in die App führen, wenn Benutzerinnen und Benutzer feststellen, dass ihre Kontodaten potentiell kompromittiert sind. Drittens kann es bei bestimmten Arten von Anwendungen, insbesondere bei solchen, die Anonymität oder Datenschutz versprechen, zu ernsthaften Datenschutzverletzungen führen.

Acht der neun Prüfungsfeststellungen bezogen sich direkt auf diesen Kontext. In einem weiteren Fall wurde ein Captcha, welches das massenhafte automatisierte Erstellen von Benutzerkonten sowie Bruteforcen der Benutzerkonten unterbinden sollte, nicht ordnungsgemäß eingebunden. Konkret wurde durch das Backend nicht geprüft, ob das Captcha (richtig) gelöst wurde. Hierdurch werden auch Benutzerenumerationen erleichtert.

4.2.2.3 Verwendung veralteter Cipher Suites und TLS-Versionen

Die Nutzung veralteter Cipher Suites und TLS-Versionen, die nicht den aktuellen Empfehlungen wie denen des BSI entsprechen, birgt erhebliche Risiken für die IT-Sicherheit. TLS, das Protokoll für sichere

Internetkommunikation, ist von entscheidender Bedeutung, und die Auswahl der Cipher Suites und Protokollversionen spielt eine wesentliche Rolle für die Integrität und Vertraulichkeit der Datenübertragung. 9 Prozent der Prüfungsfeststellungen entfallen auf diesen Themenbereich.

Ältere TLS-Versionen wie TLS 1.0 und 1.1 und veraltete Cipher Suites weisen Schwächen auf, die mittlerweile bekannt und in neueren Versionen behoben sind. Diese Schwachstellen bieten Angriffsflächen für verschiedene Exploits, wie beispielsweise den POODLE- oder BEAST-Angriff, die es Angreifern ermöglichen, verschlüsselte Daten abzufangen oder zu manipulieren. Die Verwendung solcher veralteten Standards führt nicht nur zu einer schwächeren Verschlüsselung, die leichter kompromittiert werden kann, sondern auch zu Problemen bei der Kompatibilität mit modernen Systemen, die aktuellere und sicherere Versionen voraussetzen.

Darüber hinaus können Organisationen, die veraltete TLS-Versionen und Cipher Suites verwenden, gegen Compliance-Anforderungen verstoßen. Viele Datenschutz- und Sicherheitsvorschriften verlangen die Nutzung aktueller und sicherer Verschlüsselungsmethoden. Ein Verstoß gegen diese Bestimmungen kann rechtliche Konsequenzen nach sich ziehen und das Vertrauen in die Sicherheit der Dienste untergraben.

4.2.2.4 Benutzertracking

Das IT-Sicherheitsrisiko durch Benutzertracking in Steuererklärungsapps ist besonders kritisch, da diese Apps oft sensible finanzielle und persönliche Informationen verarbeiten. Benutzertracking, welches in Form von Cookies, Tracking-Pixeln oder anderen Technologien implementiert wird, kann detaillierte Informationen über die Nutzungsgewohnheiten der Nutzenden sammeln. In Steuererklärungsapps könnten solche Daten Einblick in das Einkommen, Investitionen und andere finanzielle Aspekte der Nutzenden bieten.

Durch das Sammeln und Speichern persönlicher und finanzieller Daten innerhalb der Tracking-Systeme können detaillierte Nutzerprofile entstehen und ein wirksamer Datenschutz untergraben werden. Diese Profile sind besonders wertvoll und sensibel, da sie direkte finanzielle Informationen enthalten. Ein unzureichender Schutz dieser Daten könnte dazu führen, dass sie von Dritten eingesehen oder abgefangen werden. Dieses Risiko wird noch verstärkt, wenn Tracking-Daten außerhalb der eigentlichen App, beispielsweise auf Servern von Werbenetzwerken, gespeichert werden.

Ein weiteres Sicherheitsrisiko ist die potentielle Verwendung von Tracking-Daten für Phishing-Angriffe. Angreifer könnten die gewonnenen Informationen nutzen, um gezielte Betrugsversuche zu starten, indem sie sich beispielsweise als legitime Finanzinstitutionen oder Steuerbehörden ausgeben. Auch die Gefahr von Profilbildung und Überwachung ist in diesem Kontext besonders problematisch, da Nutzende möglicherweise nicht wissen, dass ihre finanziellen Aktivitäten verfolgt und analysiert werden.

Sieben Prüfungsfeststellungen beziehen sich auf das Benutzertracking. Dadurch sollten die Dienstanbieter für eine kritische Auseinandersetzung mit der Thematik sensibilisiert und das Hinterfragen der aktuellen Tracking Policy angeregt werden. In vier Fällen konnte das Benutzertracking durch Nutzerinnen und Nutzer gar nicht eingeschränkt werden.

4.2.2.5 Datenübermittlung an Drittanbieter

Dieser Sachverhalt trifft auf ebenfalls 7 Prozent der Prüfungsfeststellungen zu. Weitere Details hierzu sind dem Abschnitt 4.2.1.1 zu entnehmen.

4.2.2.6 Fehlende Zwei-Faktor-Authentisierung

Die fehlende Option zur Nutzung von Zwei-Faktor-Authentisierung (2FA) in Steuererklärungsapps stellt ein nennenswertes IT-Sicherheitsrisiko dar. Sechs Prozent der Prüfungsfeststellungen entfallen auf diese fehlende Option.

2FA bietet eine zusätzliche Sicherheitsebene, indem sie neben der herkömmlichen Passworteingabe eine zweite Authentifizierungsmethode, wie beispielsweise einen Code, der an das Mobiltelefon gesendet wird,

oder biometrische Daten, verlangt. Das Fehlen dieser zusätzlichen Sicherheitsmaßnahme erhöht das Risiko eines unautorisierten Zugriffs erheblich.

Ohne 2FA sind die Konten der Nutzenden hauptsächlich durch ihre Passwörter geschützt, die oft schwach sind oder wiederverwendet werden (vgl. hierzu auch 4.2.2.8). Das macht sie anfällig für eine Vielzahl von Angriffen, wie Phishing oder Brute-Force-Angriffe. Angesichts der Tatsache, dass Steuererklärungsapps Zugang zu detaillierten finanziellen Informationen bieten, kann ein erfolgreicher Angriff schwerwiegende Folgen haben, von Identitätsdiebstahl bis hin zu finanziellen Verlusten.

Darüber hinaus kann die fehlende Option zur Nutzung von 2FA in Steuererklärungsapps zu einem Vertrauensverlust bei den Nutzerinnen und Nutzern führen.

4.2.2.7 Mangelhafte Cookie-Konfiguration

6 Prozent der Prüfungsfeststellung entfallen auf eine mangelhafte Cookie-Konfiguration, insbesondere von Authentifizierungs- und Session-Cookies. Diese Cookies sind essenziell für die Aufrechterhaltung des Benutzerzustands und der Authentifizierungsinformationen in Webanwendungen. Eine unsachgemäße Handhabung kann zu verschiedenen Sicherheitsbedrohungen führen, darunter Session-Hijacking und Cross-Site Scripting (XSS).

Authentifizierungs- und Session-Cookies sollten stets mit dem Secure-Flag versehen werden. Das Secure-Flag stellt sicher, dass das Cookie nur über eine sichere HTTPS-Verbindung übermittelt wird, was das Risiko des Abfangens dieser sensiblen Cookies durch Man-in-the-Middle-Angriffe reduziert. Bei einer Übertragung über unsichere HTTP-Verbindungen können Angreifer die Cookies leicht abfangen und die Identität des Nutzenden übernehmen.

Das HTTP-Only-Flag ist eine weitere wichtige Sicherheitsmaßnahme. Wenn dieses Flag gesetzt ist, kann das Cookie nicht über clientseitige Skripte wie JavaScript zugegriffen werden. Dies verringert das Risiko von XSS-Angriffen, bei denen Angreifer versuchen, Zugriff auf Cookies zu erlangen, um sensible Informationen wie Session-IDs zu stehlen. Ohne das HTTP-Only-Flag können Cross-Site Scripting-Angriffe dazu führen, dass ein Angreifer die Kontrolle über die Sitzung eines Nutzenden erlangt.

Eine mangelhafte Cookie-Konfiguration, insbesondere das Fehlen dieser Flags, steigert das Risiko für eine Reihe von Sicherheitsbedrohungen. Authentifizierungs- und Session-Cookies ohne diese Schutzmaßnahmen sind anfällig für Interception und Missbrauch, was die Sicherheit der gesamten Webanwendung und der Benutzerdaten gefährdet.

4.2.2.8 Mangelhafte Passwortrichtlinie

Mangelhafte oder schwache Passwortrichtlinien sowie das Fehlen eines Blacklistings von häufig verwendeten oder kompromittierten Passwörtern, stellen ein erhebliches IT-Sicherheitsrisiko dar und betrifft fünf Prozent der Prüfungsfeststellungen.

Hieraus resultiert eine Anfälligkeit für Brute-Force-Angriffe. Ohne starke Passwortrichtlinien und ein Blacklisting gängiger Passwörter können einfache Passwörter oft in Sekunden oder Minuten geknackt werden. Wörterbuchangriffe, die häufig verwendete Wörter oder Phrasen nutzen, sind ebenfalls effektiver, wenn keine Komplexitätsanforderungen bestehen und gängige Passwörter nicht ausgeschlossen werden.

Ein weiteres Sicherheitsrisiko ergibt sich aus der Passwort-Wiederverwendung, bei der Nutzende dasselbe Passwort für mehrere Konten verwenden. Dieses Risiko wird durch das Fehlen eines Blacklistings von bekannten, häufig verwendeten oder in Datenlecks aufgetauchten Passwörtern verstärkt. Solche Passwörter sind oft öffentlich bekannt und bieten Angreifern eine einfache Möglichkeit, Zugriff auf mehrere Konten zu erlangen.

Phishing-Angriffe und soziale Manipulation, bei denen Nutzende zur Preisgabe ihrer Passwörter verleitet werden, sind ebenfalls problematisch.

4.3 Offenlegung der Prüfungsfeststellungen gegenüber den Dienstanbietern und Stellungnahmen

Das BSI hat die gewonnen Erkenntnisse der technischen Untersuchungen an die jeweiligen Dienstanbieter der Steuererklärungsapps übermittelt. Diese hatten anschließend vier Wochen Zeit die Prüfungsfeststellungen zu sichten, zu validieren und Rückfragen zu stellen. Ebenfalls wurde erwartet, dass die Hersteller eine Gegendarstellung oder technisch-organisatorische Maßnahmen zur weiteren Behandlung der Sachverhalte vorlegten.

Über diesen kommunikativen Ansatz verfolgt das BSI das Ziel, die Dienstanbieter weiter für den Schutzbedarf der Verbraucherdaten zu sensibilisieren und gleichzeitig die Belange aller Stakeholder zu berücksichtigen. Dienstanbieter können Prüfungsfeststellungen durchaus abweichend bewerten, da sie in der Regel ein umfangreicheres Hintergrundwissen über die genaue Funktionsweise der Anwendung verfügen. So wurden einzelne Prüfungsfeststellungen nicht weiterverfolgt und auch nicht in die Auswertung aufgenommen, wenn dem BSI plausible Erläuterungen zur Notwendigkeit von konkreten technischen Umsetzungen vorgelegt wurden. Gleichzeitig gab es Unterschiede zwischen den Produktiv- und Testsystemen, wodurch einzelne Prüfungsfeststellungen im Dialog entkräftet werden konnten.

Zum Zeitpunkt der Veröffentlichung dieses Abschlussberichts ist der Anbieterdialog durch das BSI beendet. In allen neun Fällen wurde seitens des BSI ein kooperativer, verantwortungsvoller und lösungsorientierter Reaktionsprozess verzeichnet. Kein Bestandteil des Prozesses war es, die ergriffenen Maßnahmen der Anbieter erneut technisch zu prüfen. Zudem ist es üblich, dass die Behebung von Prüfungsfeststellungen entsprechend des Risikos priorisiert wird. Es kann also nicht ausgeschlossen werden, dass die Dienstanbieter weiterhin an der Behebung arbeiten. Grundsätzlich wurde aber die Behebung aller Feststellungen der Risikograde „high“ und „medium“ angekündigt oder sogar bereits als implementiert gemeldet. Bei den Risikograden „low“ und „Info“ wird oftmals durch die Dienstanbieter eine legitime Priorisierung unter Risikogesichtspunkten vorgenommen. Aufgrund von grundlegenden Architekturentscheidungen kann eine längere Bearbeitungszeit erforderlich sein. Im Falle von Feststellungen, die lediglich als „Info“ klassifiziert sind, strebt das BSI zudem weniger eine direkte Behebung, sondern eher eine weitere Auseinandersetzung mit der Thematik an, da es sich hierbei oftmals um grundlegende Umsetzungsfragen handelt.

Von den Rückmeldungen der Dienstanbieter sollen folgende Aspekte schlaglichtartig herausgegriffen werden, da sie die Prüfungsfeststellungen ergänzen:

- **Monitoring und Schutzeinrichtungen**
  Einige Dienstanbieter haben in ihren Stellungnahmen darauf hingewiesen, dass sie zur Ermöglichung dieser technischen Untersuchung Schutzeinrichtungen abgeschaltet und Meldungen der Monitoringsysteme missachtet haben. Im Normalbetrieb wären somit also intensivere Abwehrmaßnahmen eingeleitet worden.
  Grundsätzlich wird dieser Aspekt durch das BSI positiv bewertet, da bestimmte Auswirkungen im konkreten Fall mitigiert werden können. Aus dem reinen Blick der IT-Sicherheit wird ein anderer, prinzipieller Maßstab angelegt. Eine Schwachstelle wird stets mit dem Blick auf den „worst case possible“ betrachtet. In diesem Kontext ist zu beachten, dass die Penetrationstester aufgrund des begrenzten Zeitansatzes keinerlei Augenmerk darauflegten, unerkannt zu bleiben. Ein Angreifer hat dagegen in der Regel unbegrenzt Zeit und kann beispielsweise Requests mit entsprechend langen Delays absetzen, um unerkannt zu bleiben. Eine Sperre auf IP-Ebene ist für professionelle Angreifer zudem kein nennenswertes Hindernis. Heutzutage können sich diese im Darknet für relativ geringe Geldbeträge einen Zugang zu Bot-Netzen mieten und verfügen so über unzählige IP-Adressen.
- **Beschränktes Risiko durch Gefährdung einzelner Steuererklärungen**
  Es wurde mehrfach angeführt, dass sich Prüfungsfeststellungen überwiegend auf Sachverhalte beziehen, die das Abgreifen einzelner Steuererklärungen ermöglichen können. Es handele sich damit um eher unattraktive Ziele für Angreifer. Aus Sicht der IT-Sicherheit ist jedoch der Maßstab „worst case possible“ anzulegen. Die Annahme, das Abgreifen einzelner Steuererklärungen sei für Angreifer

unattraktiv, unterschätzt gravierend die Risiken und potentiellen Konsequenzen für die IT-Sicherheit. Zunächst sind einzelne Steuererklärungen für Cyberkriminelle von erheblichem Wert, da sie detaillierte persönliche und finanzielle Informationen enthalten. Diese Daten können für Identitätsdiebstahl, Betrug oder Erpressung missbraucht werden, was ihren Marktwert beträchtlich steigert. Darüber hinaus können die kumulativen Auswirkungen solcher Angriffe erheblich sein; selbst wenn zunächst nur einzelne Accounts betroffen sind, könnte sich dies zu einem umfangreicheren Datenleck entwickeln. Zudem findet angreiferseitig eine stete Professionalisierung statt, die unter anderem mit einer Automatisierung der Angriffe einhergeht, ggf. mit Unterstützung durch sogenannte Künstliche Intelligenz.
Neben den direkten Risiken für die betroffenen Individuen können solche Sicherheitsvorfälle auch das Vertrauen in die betroffene Plattform untergraben und zu langfristigen Reputationsschäden führen. Außerdem dürfen die rechtlichen und regulatorischen Konsequenzen von Datenschutzverletzungen nicht unterschätzt werden. Angesichts strenger Datenschutzgesetze wie der DSGVO können solche Verstöße zu erheblichen rechtlichen Konsequenzen führen. Insgesamt ist es daher unerlässlich, alle notwendigen Sicherheitsmaßnahmen zu ergreifen, um die Daten zu schützen und das Risiko von Cyberangriffen zu minimieren. Die Annahme, dass das Abgreifen einzelner Steuererklärungen für Angreifer unattraktiv sei, verkennt somit die Realitäten und Gefahren der modernen IT-Sicherheitslandschaft.

- **Zwei-Faktor-Authentisierung**
  Zur Thematik der 2FA gab es von den Dienstanbietern durchweg positive Rückmeldungen hinsichtlich der Planung einer Einführung oder zumindest einer Machbarkeitsuntersuchung. Den Stellungnahmen konnte teilweise entnommen werden, dass dessen Implementierung als tiefgreifende Architekturentscheidung verstanden werden muss und insbesondere die Aspekte der Usability und Akzeptanz bei den Nutzenden aus ökonomischer Sicht für die Unternehmen eine gewisse Herausforderung darstellen. Denn die Akzeptanz in der Zielgruppe ist letztlich die Voraussetzung für eine langfristige Etablierung und Marktdurchdringung der 2FA. Mit Blick auf die Ergebnisse des Cybersicherheitsmonitors 2023 ist dieses Verfahren zumindest bei 50 % der befragten Personen bekannt und wird von 42 % aktiv genutzt.[4]
  In diesem Zusammenhang sind einige Stellungnahmen ebenfalls positiv hervorzuheben, die von geplanten Überprüfungen der genutzten Authentisierungsverfahren mit Berücksichtigung einer Implementierung von Passkeys berichten.

- **Cipher-Suites und TLS-Versionen von Drittanbietern abhängig**
  Die Prüfungsfeststellungen zu veralteten Cipher-Suites und TLS-Versionen wurden nach Auskunft der Dienstanbieter gewissenhaft geprüft und sofern in direkter eigener Zuständigkeit liegend zeitnah bearbeitet. Ein anderes Bild ergibt sich, wenn veraltete Cipher-Suites und TLS-Versionen aus der Kommunikation mit Endpunkten in Verantwortung von Drittanbietern resultieren. In drei Fällen gaben die Unternehmen an, dass sie Drittanbieter mit der Bitte um Umstellung kontaktiert haben und ggf. die Nutzung alternativer Dienstleister prüfen. In 4 Fällen hingegen bezogen sich die Unternehmen auf die Zuständigkeit der Dienstleister und der fehlenden Einflussmöglichkeiten. Selbst bei einem kostenintensiven Austausch des Dienstleisters kann für die Zukunft nicht sichergestellt werden, dass dieser regelkonform bleibt.
  Nach Auffassung des BSI verkennt diese Haltung die beim Dienstanbieter liegende Gesamtverantwortung für die Daten- und IT-Sicherheit deutlich.

- **Tracking**
  Auch bei diesem Punkt ist positiv zu verzeichnen, dass die Dienstanbieter mit den Prüfungsfeststellungen verantwortungsvoll umgehen und sich der Thematik annehmen. Die Stellungnahmen machten deutlich, dass sich die Unternehmen mit der Behebung angabegemäß

[4] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2023_Folien.pdf?__blob=publicationFile&v=2

gewissenhaft auseinandersetzen werden bzw. die Bearbeitung bereits vor den Prüfungsfeststellungen begonnen haben und man aktuell vor einer grundsätzlichen Überarbeitung steht.
Grundsätzlich bleibt hier abzuwarten, wie sich dies für die Nutzerinnen und Nutzer in der Praxis auswirkt, da sich die Prüfungsfeststellungen überwiegend auch auf das Einwilligungsmanagement bezogen. Hier bestehen in gewisser Weise Interessenskonflikte, die immer wieder zur Nutzung sogenannter Dark Pattern führen. Die konkrete Bewertung solcher Sachverhalte entziehen sich jedoch der Zuständigkeit des BSI.

5 Schlussfolgerungen aus der technischen Untersuchung

5.1 Vergleich mit früheren Untersuchungen dieser Publikationsreihe

Bereits im Jahr 2021 hat das BSI eine technische Untersuchung von Gesundheitsapps veröffentlicht.[5] Auch wenn sich das durchgeführte Prüfprogramm dieser beiden Untersuchungen unterscheidet, soll an dieser Stelle kurz beleuchtet werden, ob es Auffälligkeiten bei den Prüfungsfeststellungen zwischen den Gesundheitsapps und den Steuererklärungsapps gibt, da es sich technisch gesehen um eine vergleichbare Produktkategorie (hier: Apps) handelt und in beiden äußerst sensible personenbezogene Daten verarbeitet werden.

Bei den Gesundheitsapps waren die maßgeblichen Feststellungen:

- Mangelhafter Umgang mit Passwörtern (Passwortübertragung im Klartext)
- Erhöhtes Risiko möglicher Angriffsszenarien durch hohe Komplexität der Architektur, also durch umfangreiche Nutzung von Drittanbieter-Dienstleistungen im Cloudumfeld
- Nutzung veralteter Verschlüsselungsmechanismen
- Anfälligkeit für Man-in-the-Middle-Angriff
- Fehlende Inhaltsverschlüsselung ergänzend zur Transportverschlüsselung in der Kommunikation zwischen Client und Backend

Entsprechend des Aggregationsniveaus lässt sich erkenne, dass sich das Segment der Steuererklärungsapps im Vergleich zu den Gesundheitsapps weder positiv, noch negativ abhebt. Es sind gewisse Parallelen zwischen den Clustern der Prüfungsfeststellungen zu verzeichnen, auch wenn es beispielsweise bei den potentiellen Angriffsszenarien Unterschiede gibt (MitM versus XSS und Benutzerenumeration).

5.2 Forderungen aus Sicht des Digitalen Verbraucherschutzes

Die Ergebnisse der technischen Untersuchung unterstreichen wesentliche Forderungen des Digitalen Verbraucherschutzes an die Hersteller und Anbieter von Verbraucherprodukten und -diensten. Diese Forderungen zahlen im Wesentlichen auf die Konzepte Security by Design, Security by Default und Usable Security ein. Im Folgenden werden die Forderungen in Bezug auf die Prüfungsfeststellungen auszugsweise aufgeführt:

- **Periodische Überprüfung der Verschlüsselungsverfahren**
  Aufgrund der rasanten technologischen Entwicklung und potentiellen Schwachstellen in älteren Verfahren sollten Hersteller regelmäßige Überprüfungen und daraus abgeleitete Updates ihrer Verschlüsselungsstrategien durchführen.
  Ein adäquater Schutz der Daten, sei es im Speicher oder während der Übertragung, ist fundamental, um das Vertrauen und die Sicherheit der Verbraucherinnen und Verbraucher zu gewährleisten. Diese Forderungen reflektieren das Bedürfnis nach einem umfassenden Datenschutz und Sicherheit persönlicher Informationen. Ein angemessenes Verschlüsselungsmanagement stärkt das Vertrauen und gewährleistet die Integrität und Vertraulichkeit der Daten. Es ist dabei nicht nur eine Frage der Technologie, sondern auch eine Frage der Ethik und Verantwortung gegenüber den Nutzenden. Jeder Verstoß oder Missbrauch kann erhebliche Auswirkungen auf die Reputation und das Vertrauen in ein Unternehmen oder Produkt haben. Daher sollte die Sicherheit der genutzten

[5] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.html?nn=132496#download=0

Verschlüsselungsverfahren als eine der höchsten Prioritäten in jeder IT-Sicherheitsstrategie betrachtet werden.

- **Anmeldungen bei Diensten**
  Es sollte sichergestellt werden, dass nur autorisierte Personen auf Daten zugreifen können. Dies kann durch die Implementierung von Multi-Faktor-Authentisierung, Biometrie, Passwortrichtlinien und regelmäßige Überprüfungen von Zugriffsrechten erreicht werden. OAuth und OpenID sind gängige Standards für sichere Authentifizierung und Autorisierung. Insbesondere wird gefordert:
  - Starke Passwörter: Passwortregeln müssen dem aktuellen Stand der Technik entsprechen.
  - eine 2FA muss angeboten werden. Diese sollte ein sicheres Verfahren nutzen.[6]
  - eine Zwei-Faktor-Authentisierung sollte auf zwei voneinander getrennten Geräten erfolgen; eine 2FA auf einem Gerät ist keine "echte" 2FA.
- **Regelmäßige Sicherheitsüberprüfungen**
  In einer sich rasant entwickelnden digitalen Welt ist es nicht ausreichend, Sicherheitsüberprüfungen für Verbraucherprodukte und -dienste nur einmalig bei der Markteinführung durchzuführen. Neue Bedrohungen, Angriffsvektoren und Schwachstellen können im Laufe der Zeit entstehen und bestehende Sicherheitsmaßnahmen unwirksam machen. Daher ist es von zentraler Bedeutung, dass Hersteller und Dienstanbieter ihre Produkte und Services regelmäßig auf IT-Sicherheit überprüfen.
  - Hersteller und Dienstanbieter müssen ihre Produkte und Services daher regelmäßig einer Sicherheitsüberprüfung unterziehen. Der Turnus sollte dabei risikoorientiert gewählt werden.
  - Externe Sicherheitsexperten oder Organisationen sollten in den Überprüfungsprozess einbezogen werden, um eine objektive und unvoreingenommene Bewertung zu gewährleisten.
  - Das interne Team sollte regelmäßig in Bezug auf neue Sicherheitsbedrohungen und -technologien geschult werden, um auf dem neuesten Stand zu bleiben.
  - Automatisierte Sicherheitsüberprüfungen können teilweise genutzt werden, um Effizienz und Konsistenz zu gewährleisten, müssen aber durch weitere Aspekte ergänzt werden.
  - Sicherheitsüberprüfungen müssen fest in den Entwicklungszyklus von Produkten und Dienstleistungen integriert werden, sodass jede neue Version oder Aktualisierung automatisch überprüft wird.
  - Es sollte ein "Bug-Bounty"-Programm angeboten werden.
- **Sicherheitsbewertung von Drittanbietern**
  In der heutigen digitalen Landschaft sind viele Verbraucherprodukte und -dienste nicht isoliert, sondern setzen sich aus einer Vielzahl von Komponenten zusammen, die oft von Drittanbietern stammen. Diese Komponenten können Betriebssysteme, Softwarebibliotheken, Hardwaremodule oder Cloud-Dienste sein. Während diese Integrationen oftmals die Funktionalität und den Nutzen für Verbraucherinnen und Verbraucher erhöhen, bringen sie auch zusätzliche Sicherheitsrisiken mit sich.
  - Hersteller von Verbraucherprodukten und -diensten müssen sicherstellen, dass alle integrierten Drittanbieterkomponenten den gleichen hohen Sicherheitsstandards entsprechen, wie die Produkte und Dienstleistungen in denen sie eingebunden sind.
  - Regelmäßige Überprüfungen: Vor der Integration sollte eine gründliche Sicherheitsüberprüfung der Drittanbieterkomponenten stattfinden. Dies umfasst sowohl eine technische Überprüfung als auch die Bewertung des Anbieters in Bezug auf dessen Reputation in Fragen der IT-Sicherheit.

[6] Ergänzende Informationen zur technischen Betrachtung von 2FA-Verfahren finden sich hier: https://www.bsi.bund.de/dok/11693908

- Aktualisierungen und Patches: Hersteller müssen sicherstellen, dass sie über alle Sicherheitsupdates und Patches für die Drittanbieterkomponenten umgehend im Bilde sind und diese zeitnah einspielen können.
- Vereinbarungen zur Sicherheitsverantwortung: Bei der Zusammenarbeit mit Drittanbietern sollten klare Vereinbarungen über die Verantwortlichkeiten in Bezug auf IT-Sicherheitsfragen getroffen werden.
- Die Integration von Drittanbieterkomponenten sollte nicht auf Kosten der Sicherheit gehen. Durch die Berücksichtigung der genannten Forderungen können Hersteller die Risiken minimieren und gleichzeitig den Nutzen für Verbraucherinnen und Verbraucher maximieren.

- **Datensparsamkeit und Zweckbindung**
  In einer digital vernetzten Welt, in der Daten oft als "das neue Gold" bezeichnet werden, ist der Schutz personenbezogener Informationen unerlässlich. Dabei stehen nicht nur der Missbrauch von Daten oder der Datendiebstahl im Fokus, sondern ebenso die datenschutzrechtlichen Verpflichtungen und das Grundrecht auf informationelle Selbstbestimmung. Beim Schutz der Daten spielen daher sowohl eine ethische, als auch eine rechtliche Perspektive eine wesentliche Rolle. Das Prinzip der Datensparsamkeit ist dabei eine Schlüsselstrategie, um diesen Schutz zu gewährleisten.
  - Verbraucherprodukte und -dienste müssen die Grundsätze der Datensparsamkeit und Zweckbindung berücksichtigen. Es sind nur die Daten zu erheben und zu verarbeiten, die für den spezifischen Zweck des Produkts oder Dienstes erforderlich sind.
  - Unternehmen müssen vor der Datenerhebung bewerten, welche Daten wirklich notwendig sind.
  - Unternehmen müssen klare Richtlinien und Verfahren für die regelmäßige Überprüfung und Löschung von nicht mehr benötigten Daten haben.

5.3 Corporate Digital Responsibility (CDR)

Corporate Digital Responsibility (CDR) steht als freiwillige Selbstverpflichtung für ein verantwortungsvolles Handeln von Unternehmen in der digitalen Gesellschaft, dass über die Erfüllung von gesetzlichen Anforderungen und Standards hinausgeht. Durch den Digitalisierungsschub der letzten Jahre hat die Verantwortung und das Bewusstsein, IT-Sicherheit bereits bei der Entwicklung und Gestaltung digitaler Produkte und Dienstleistungen sowie über den gesamten Produktlebenszyklus zu berücksichtigen, zunehmend an Relevanz gewonnen. Hiermit wird die bereits seit geraumer Zeit diskutierte „Corporate Social Responsibility“ als sozial, gesellschaftlich und ökologisch verantwortungsvolles Unternehmenshandeln um den Aspekt der digitalen Verantwortung erweitert.

Unternehmen handeln dann verantwortungsvoll, wenn sie sorgfältig mit den Daten ihrer Nutzerinnen und Nutzer umgehen, diese sicher verwalten und vor Angriffen bzw. unkontrollierten Abflüssen schützen. Im Kontext von Steuererklärungapps heißt dies, einen ständigen Blick darauf zu haben, welche Daten verarbeitet werden und ob durch eine Erweiterung des Funktionsumfangs der App eine Erweiterung des Schutzes der Nutzerdaten angezeigt ist. Hierzu zählt auch das Bekenntnis der Dienstanbieter zur Bereitstellung regelmäßiger und zeitnaher Sicherheitsaktualisierungen während des gesamten Produktlebenszyklus. Gerade bei Steuererklärungsapps, welche einen gewissen Lock-in-Effekt haben, besteht hier aus Sicht des BSI eine besondere Verantwortung der Unternehmen. Dieser Kundenbindungseffekt besteht grundsätzlich durch die jährlich wiederkehrende Aufgabe der Erstellung einer Steuererklärung, aber insbesondere durch die Übernahme von Angaben der Steuererklärung aus dem Vorjahr, sodass der Prozess erleichtert und beschleunigt wird.

Teilweise wurde dem BSI in den Stellungnahmen mitgeteilt, dass man sich des Sachverhalts annehmen werde, auch wenn es hierfür keine regulatorische Anforderung gäbe. Bereits an dieser Stelle beginnt CDR, auch ohne jedwede Regulatorik. Angesichts der Sensibilität der Daten, die in Steuererklärungsapps verarbeitet werden – darunter Einkommensinformationen, Sozialversicherungsnummern,

Steueridentifikationsnummern und andere persönliche Identifikatoren – ist die Gewährleistung der Datensicherheit nicht nur eine Frage der Compliance, sondern auch ethisch geboten. Zudem ist mit relevanten Reputationsschäden für die Unternehmen im Fall eines Sicherheitsvorfalls zu rechnen. Im Cybersicherheitsmonitor 2023 nannten von Internetkriminalität Betroffene mit 33 % den Vertrauensverlust in entsprechende Online-Dienste als häufigsten Schaden.[7]

Durch fortlaufende Investitionen in die IT-Sicherheit der eigenen Produkte und Dienste sowie der verantwortungsvollen Behebung von Prüfungsfeststellungen bietet sich den Unternehmen die Chance, ihre eigene Marktpositionierung und -stellung zu verbessern. Die Umsetzung konkreter IT-Sicherheitsmaßnahmen bildet eine wichtige Grundvoraussetzung für Vertrauen.

Wie bereits eingangs erwähnt: Auch im Rahmen dieser technischen Untersuchung wirkte der kooperative Dialog mit den Dienstanbietern. Alle beteiligten Unternehmen haben offen und fachlich fundiert mit dem BSI zusammengearbeitet, sodass im Ergebnis die IT-Sicherheit im Bereich der Steuererklärungsapps spürbar vorangebracht werden konnte. Dieser kooperative Ansatz ist als verantwortungsvolles Handeln von Unternehmen ein Vorbild für praktizierte Corporate Digital Responsibility und aus Sicht des BSI ein wichtiger Baustein für den aktiven Schutz der Menschen in der digitalen Welt.

[7] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2023_Folien.pdf?__blob=publicationFile&v=2

Literaturverzeichnis

Bitkom e.V. 2023. *6 von 10 Steuererklärungen wurden zuletzt online abgegeben.* URL: https://www.bitkom.org/Presse/Presseinformation/6-von-10-Steuererklaerungen-zuletzt-online-abgegeben

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. *IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps.* URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.html?nn=132496#download=0

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2023. *Der Cybersicherheitsmonitor: Bürgerbefragung zur Cybersicherheit 2023.* URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2023_Folien.pdf?__blob=publicationFile&v=2

FIRST.ORG, Inc. *Common Vulnerability Scoring System Calculator.* URL: https://www.first.org/cvss/calculator/3.1