Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Passwortmanager

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	01.12.2025	BSI und FZI	Erste Version

Tabelle 1: Änderungshistorie

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

IT-SICHERHEIT AUF DEM DIGITALEN VERBRAUCHERMARKT:

Fokus Passwortmanager

Zentrale Prüffeststellungen

- Bei der Mehrzahl der Produkte liegen keine öffentlich verfügbaren Informationen über Sicherheitsauditierungen oder Penetration-Tests vor.
- Nach Änderung des Masterpassworts erfolgt bei acht von zehn Passwortmanagern keine vollständige Neuverschlüsselung des Passwort-Containers.
- Lediglich 4 der untersuchten Passwortmanager setzen sichere, korrekt konfigurierte kryptografische Algorithmen ein.
- Lediglich bei 3 der untersuchten Produkte wird der komplette Inhalt verschlüsselt.
- Bei 3 von 10 der untersuchten Produkte werden die Passwörter so abgelegt, dass Hersteller theoretisch darauf zugreifen könnten.

Die Prüffeststellungen beziehen sich auf die jeweils im Bericht getestete Version

Bundesamt
für Sicherheit in der
Informationstechnik

Warum ist ein Passwortmanager wichtig für Dich?

Ein Passwortmanager unterstützt Dich dabei starke Passwörter für Deine Onlineaccounts zu generieren, diese verschlüsselt zu speichern, vor unsicheren Websites und Phishing-Attacken zu warnen. Einige Programme können die Nutzung auf mehreren Geräten komfortabel synchronisieren.

Untersuchte Produkte

1Password

Avira Password Manager

Mozilla Firefox Password Manager

mSecure Password Manager

Google Chrome Password Manager

PassSecurium

SecureSafe Password Manager

KeePass2Android

KeePassXC

S-Trust Password Manager

Empfehlungen für Dich

- Wähle einen Passwortmanager aus
- Richte immer ein starkes Masterpasswort ein
- Nutze eingebaute Backup-Funktionen oder sichere Deine Daten manuell
- Doppelt absichern – Aktiviere Zwei-Faktor-Authentisierung, am besten mit Hardware-Token oder TOTP
- Sorge dafür, dass Dein Passwortmanager nach einer Inaktivität gesperrt wird

Vergleichstabelle der untersuchten Passwortmanager

Produkt	1 Password	Avira Password Manager	Chrome Password Manager	Keepass2 Android	KeePassXC	Mozilla Firefox Password Manager	mSecure-Password Manager	PassSecurium	SecureSafe Password-Manger	S-Trust Password Manger
Untersuchte Version	Version 8.10.62 für Android	Version 2.11 für Android	Version 137.0.7151.69 unter Windows 10 Pro	Version 1.12-r5 für Android	Version 2.7.9 für Windows	Version 139.0.1 für Windows	Version 6.1.5 für Android	Privatkunden-Tarife FREE/Standard; Android 1.1.63 / iOS 2.1.2	2.24.1 für Windows.	Version 4.0.1 für Windows.
Sicherheitstechnische Eigenschaften										
Verwendung eines Masterpassworts in der Standardkonfiguration	Ja	Ja	Ja[1]	Ja	Ja	Nein	Ja	Ja	Ja	Ja
Wiederherstellungsoption bei Verlust des Masterpassworts	Ja	Nein[2]	Nein[3]	Nein	Nein	Ja	Nein	Ja	Ja	Ja
Kann mit zweitem Faktor geschützt werden	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

[1] Anstelle des Masterpassworts wird die Windows-Authentifizierung verwendet, dies ist in diesem Kontext vergleichbar.
[2] Die vorhandene Wiederherstellungsoption über Biometrie sollte aus Sicherheitsgründen deaktiviert werden, Details dazu in Abschnitt 5.2.2.
[3] Nutzende sollten eine eigene Passphrase setzen, eine Wiederherstellungsoption ist dann nicht mehr vorhanden, Details dazu in Abschnitt 5.2.3.

Produkt	1 Password	Avira Password Manager	Chrome Password Manager	Keepass2 Android	KeePassXC	Mozilla Firefox Password Manager	mSecure-Password Manager	PassSecurium	SecureSafe Password-Manger	S-Trust Password Manger
Unterstützt Verwaltung zweiter Faktoren[4]	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Nein	Nein
Automatisches Leeren der Zwischenablage	Ja[5]	Ja	Nein	Ja	Ja	Nein	Ja[5]	Nein	Ja	Ja
Automatische Sperre nach Zeitüberschreitung in der Standardkonfiguration	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja
Cloud-Synchronisation[6]	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja
Prüfung gegen Leaks	Ja	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Nein	Nein
Export von Passwörtern	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Zentrale Prüffeststellung										
Der komplette Inhalt wird verschlüsselt.	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
Nach Änderung des Masterpassworts wird der komplette Inhalt verschlüsselt.	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein

[4] Verwaltung von zusätzlichen Authentisierungsfaktoren für 2FA bei anderen Diensten.
[5] Wird bei aktuellen Android Versionen vom Betriebssystem übernommen.
[6] Können gespeicherte Daten über eine einfach aktivierbare Funktion mit einer vom Hersteller oder Drittanbieter betriebenen Cloud synchronisiert werden?

Produkt	1 Password	Avira Password Manager	Chrome Password Manager	Keepass2 Android	KeePassXC	Mozilla Firefox Password Manager	mSecure-Password Manager	PassSecurium	SecureSafe Password-Manger	S-Trust Password Manger
Hersteller kann auf die Daten zugreifen.[7]	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Ja	Nicht bewertbar	Nicht bewertbar
Es werden ausschließlich sichere, korrekt konfigurierte kryptografische Algorithmen eingesetzt.[8]	Ja, mit geringen Abweichungen	Unbekannt[9]	Unbekannt, nutzt Betriebssystemfunktionen	Ja, mit geringen Abweichungen	Ja, mit geringen Abweichungen	Ja, mit geringen Abweichungen	Unbekannt, mindestens geringe Abweichungen	Nein	Nein	Nein

Tabelle 2 Vergleich getesteter Passwortmanager

[7] Details dazu in Abschnitt 4.1; die Einträge beziehen sich auf die Standardkonfiguration bei aktivierter Synchronisation.
[8] Im Sinne der BSI TR-02102-1. Details dazu in Abschnitt 4.3.
[9] Einige Informationen konnten im Rahmen der Prüftiefe nicht erhoben werden. Details dazu in den jeweiligen produktspezifischen Ergebnissen in Abschnitt 5.2.2.

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

1 Vorbemerkungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt als zentrale Cybersicherheitsbehörde des Bundes und unabhängige Stelle für den Digitalen Verbraucherschutz in Deutschland eine entscheidende Rolle für den aktiven Schutz der Menschen in der digitalen Welt ein. Zu diesem Zweck untersucht das BSI im Rahmen der Marktbeobachtung in regelmäßigen Abständen einzelne Segmente des digitalen Verbrauchermarktes mit einer tiefergehenden Analyse. Ziel ist die Identifizierung von Handlungsbedarfen auf Basis der gewonnenen Erkenntnisse, sowie die Schaffung einer Grundlage für die weitere Diskussion und Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft.

Die Publikationsreihe „IT-Sicherheit auf dem digitalen Verbrauchermarkt“ bildet dabei die zentrale Veröffentlichung der Marktbeobachtung und des Technischen Verbraucherschutzes des BSI und erscheint seit 2021 mit verschiedenen Fokusthemen, darunter: Onlineshopping-Plattformen, smarte Heizkörperthermostate, Gesundheits- und Steuererklärungsapps. Alle Berichte sind unter folgendem Link zu finden: IT-Sicherheit auf dem digitalen Verbrauchermarkt.

Damit trägt die Marktbeobachtung zur ganzheitlichen Gestaltung eines effektiven Digitalen Verbraucherschutzes in Deutschland und Europa bei. Mit einer kooperativen Umsetzung unserer Aktivitäten gemeinsam mit den Herstellern erhöht das BSI die IT-Sicherheit für konkrete Produkte und Dienste im Verbraucheralltag.

Der vorliegende Bericht bezieht sich auf die Produktgruppe der Passwortmanager. Nahezu alle beteiligten Unternehmen haben offen und fachlich fundiert mit dem BSI und dem vom BSI beauftragten Projektpartner, dem FZI Forschungszentrum Informatik, zusammengearbeitet, sodass im Ergebnis die IT-Sicherheit im Bereich der Passwortmanager vorangebracht werden konnte. Weitere Impulse setzt das BSI mit der Veröffentlichung dieses Abschlussberichts und mit der gezielten Adressierung der im Bereich dieses Untersuchungsscopes tätigen Wirtschaftsakteure.

2 Hintergrund, Ziel und Vorgehensweise

Passwörter begleiten den Alltag von Verbraucherinnen und Verbrauchern – sie sind für die Nutzung zahlreicher Onlinedienste, wie z. B. Onlineshopping, Social Media oder die Nutzung von E-Maildiensten, erforderlich. Die Notwendigkeit der Absicherung von Onlineaccounts ergibt sich aus den nahezu täglichen Meldungen über Datenleaks. Der unbefugte Zugriff auf und die Offenlegung von Daten, wie z. B. Login-Daten, erhöhen das Risiko für Verbraucherinnen und Verbraucher, Opfer von Phishing-Angriffen oder Identitätsdiebstahl zu werden.

Eine Möglichkeit der Passwortverwaltung und damit ein wichtiger Beitrag zur Absicherung von Onlineaccounts sind Passwortmanager. Doch eine im Rahmen der Accountschutz-Studie[10] durchgeführte Befragung offenbarte, dass die Verwendung von Passwortmanagern bei Verbraucherinnen und Verbrauchern oftmals auf Misstrauen stößt und Bedenken in Bezug auf deren Sicherheit bestehen. Darüber hinaus unterminieren Meldungen über Sicherheitslücken und -vorfälle bei Anbietern von Passwortmanagern das Vertrauen in die Sicherheit dieser Produkte.

Ziel der Untersuchung war es, die IT-Sicherheit verschiedener Produkte aus dem Segment der Passwortmanager zu analysieren und zu bewerten. Hierfür hat das BSI in einem ersten Schritt nach einer systematischen Marktanalyse zehn Produkte ausgewählt. Das Vorgehen zur Marktsichtung und Auswahl der Produkte ist in Kapitel 3 näher erläutert. Die ausgewählten Produkte wurden anschließend einer Gefährdungsanalyse unterzogen. Das Prüfschema für die Gefährdungsanalyse ist in Anhang: Prüfschema ersichtlich. Nach Abschluss der Untersuchung hat das BSI die jeweiligen Ergebnisberichte an die Hersteller übermittelt. Alle Hersteller hatten die Gelegenheit zu den Ergebnissen der Untersuchung Stellung zu nehmen.

Durch die gewonnenen Erkenntnisse der Gefährdungsanalyse hat das BSI die Informationslage in Bezug auf die Sicherheitseigenschaften verschiedener Passwortmanager verbessert und Risiken für Verbraucherinnen und Verbraucher bei der Nutzung dieser Produkte identifiziert.

Diese Publikation enthält einerseits Handlungsempfehlungen für Hersteller und gibt andererseits Verbraucherinnen und Verbrauchern mehr Orientierung und Sicherheit bei der Entscheidung für einen Passwortmanager.

Wichtiger Hinweis zur Interpretation der Ergebnisse

Die Berichtsergebnisse dieses Dokuments beziehen sich ausdrücklich auf die ausgewiesenen Versionsstände der untersuchten Produkte bzw. Dienste. Der begleitende Austausch dieser Erkenntnisse mit den betroffenen Unternehmen führt regelmäßig zu Produktnachbesserungen und dahingehend zur Erhöhung der IT-Sicherheit. Dies ist vordergründiges Ziel dieser Untersuchungsreihe. Aufgrund der Zeitgebundenheit dieses Berichts ist es leider nicht möglich, derartige Nachbesserungen fachlich zu prüfen und zu würdigen.

[10] Eine gemeinsame Untersuchung des Bundeskanzleramtes und des BSI zum Schutz von Onlinekonten, unter: https://www.bsi.bund.de/dok/131376 (abgerufen am 16.09.2025)

3 Marktanalyse

3.1 Marktsichtung

Im zweiten Quartal 2024 fand im Rahmen der Marktbeobachtung durch das BSI eine Analyse über die zum Projektzeitraum auf dem deutschen Markt erhältlichen Passwortmanager-Produkte statt. Basierend auf dieser Recherche wurden die Produkte anhand der folgenden Kriterien eingegrenzt:

Passwortverwaltung für den Privatgebrauch: eigenständiges Passwortmanager-Programm und browserintegrierte Passwortmanager

Entscheidend für das erste Kriterium der Produktauswahl war, dass die Anwendung eine Passwortverwaltung für den Privatgebrauch bereitstellt. Die Begrenzung auf Anwendungen für den Privatgebrauch ermöglichte eine wirksame Betrachtung des Verbrauchermarktes. Des Weiteren war relevant, dass es sich bei der Anwendung um ein eigenständiges Passwortmanager-Produkt handelt oder in einen am Verbrauchermarkt verfügbaren Browser integriert ist. Die Berücksichtigung von browserintegrierten Passwortmanagern ist dadurch begründet, dass Verbraucherinnen und Verbraucher häufig erstmals durch Browser mit der Passwortverwaltung ihrer Onlinekonten in Kontakt kommen. Die Hinzunahme dieser Anwendungen war von entscheidender Bedeutung, um Ableitungen für das gesamte Produktsegment der Passwortmanager im Verbrauchermarkt treffen zu können. Betriebssystemintegrierte Browser, die von den marktbeherrschenden Betriebssystem-Anbietern standardmäßig vorinstalliert sind, wurden nicht einbezogen. Da durch deren Berücksichtigung umfangreiche zusätzliche Tests erforderlich gewesen wären, wurden aus diesen Gründen betriebssystemintegrierte Passwortmanager nicht in die Marktanalyse einbezogen. Ebenfalls nicht berücksichtigt wurden spezialisierte Browser (z. B. textbasierte Browser), da diese teils sehr eingeschränkte Funktionalitäten anbieten. Darüber hinaus war relevant, dass die zu untersuchenden Produkte für einen einheitlichen technischen Untersuchungsaufbau geeignet sind und die erforderliche fachliche Vergleichbarkeit nach sachlichen, objektiven und nachvollziehbaren Kriterien gegeben ist.

Die Anwendung ist ausgereift ("mature software") und wurde zuletzt vor höchstens einem Jahr einem Update unterzogen

Im Rahmen der weiteren Marktanalyse war für das zweite Auswahlkriterium relevant, dass die Anwendungen im Sinne des "Software Release Life Cycle" so ausgereift sind, dass sie nach hiesiger Facheinschätzung als "stable release" angesehen werden können. Nur ab diesem Reifegrad werden Anwendungen als grundsätzlich geeignet für die Inverkehrbringung auf dem Verbrauchermarkt angesehen. Darüber hinaus wurden Anwendungen nicht berücksichtigt, deren letztes Update zum Zeitpunkt der Marktanalyse älter als 12 Monate war. Die während der Marksichtung verfügbaren Angaben boten zwar einen Hinweis über den Status der aktiven Pflege, konnten aber keine Unterscheidung nach Art der Updates liefern (z.B. Sicherheits-, Funktions- und Layout-Updates oder Updates durch Änderungen in Software-Frameworks). Es wurde die Annahme getroffen, dass sicherheitsrelevante Updates mit enthalten sind.

Die Anwendung ist plattformübergreifend verfügbar und hat eine ausreichend hohe Marktabdeckung

Ausgangsbasis für das dritte Auswahlkriterium war die Recherche nach der Verteilung der Marktanteile für Betriebssysteme von Desktop-PCs (inkl. Laptop) und Smartphone (für eigenständige Passwortmanager-Programme) sowie die Verbreitung von Internetbrowsern (browserintegrierte Passwortmanager).

Die Marktanteile der Desktop-Betriebssysteme am deutschen Verbrauchermarkt im Juli 2024 beliefen sich auf[11]:

- 76,4 % Windows
- 13,5 % OS X

[11] StatCounter (2024): Desktop Operating System Market Share Germany, unter: https://gs.statcounter.com/os-market-share/desktop/germany/#monthly-202407-202407-bar (abgerufen am 14.09.2024)

- 4,8 % Linux
- 3,8 % Unbekannt
- 1,6 % Chrome OS

Die Marktanteile der mobilen Betriebssysteme am Absatz von Smartphones am deutschen Verbrauchermarkt im 1. Quartal 2024 beliefen sich auf[12]:

- 66,1 % Android
- 33,2 % iOS
- 0,7 % andere

Um eine möglichst breite Marktabdeckung zu erreichen, war die Voraussetzung, dass die Anwendungen mobil für iOS und Android sowie für Windows und macOS plattformübergreifend verfügbar sein müssen. Auch wenn die technische Bewertung bestimmter Anwendungen auf unterschiedlichen Plattformen differenziert ausfallen kann, geben die Ergebnisse eine Orientierung in Bezug auf die IT-Sicherheit der untersuchten Passwortmanager-Programme.

Die Marktanteile der in Deutschland genutzten Internetbrowser im Juli 2024 verteilen sich wie folgt[13]:

- 46 % Chrome
- 22 % Firefox
- 18 % Edge
- 8,5 % Safari
- 4, 8 % Opera
- 0,7 % andere

Die Anwendung ist über vertrauenswürdige Bezugskanäle erhältlich

Das BSI empfiehlt Verbraucherinnen und Verbrauchern, Anwendungen ausschließlich aus vertrauenswürdigen Quellen zu beziehen[14]. Hierzu zählen die einschlägigen Hersteller- und Vertriebsplattformen bzw. App Stores am Verbrauchermarkt, die durch ihr Quasimonopol über eine nahezu vollständige Marktabdeckung verfügen und dementsprechend von Verbraucherinnen und Verbrauchern am häufigsten genutzt werden.

Folgende Produkte aus dem Segment der Passwortmanager waren nach der Anwendung der o. g. vier Kriterien in der Vorauswahl:

Eigenständige Passwortmanager-Programme

- 1Password
- 1 Passwort Manager Safe: Liso
- AuthPass – Passwort Manager
- Avira Passwort Manager

[12] Kantar (2024): Marktanteile der mobilen Betriebssysteme am Absatz von Smartphones in ausgewählten Ländern im 1. Quartal 2024. Statista, unter: https://de.statista.com/statistik/daten/studie/198453/umfrage/marktanteile-der-smartphone-betriebssysteme-am-absatz-in-ausgewaehlten-laendern (abgerufen am 16.08.2024)

[13] https://de.statista.com/statistik/daten/studie/157944/umfrage/marktanteile-der-browser-bei-der-internetnutzung-weltweit-seit-2009/ (abgerufen am 16.08.2024)

[14] https://www.bsi.bund.de/dok/6687234; https://www.bsi.bund.de/dok/6596284; https://www.bsi.bund.de/dok/1143642 (abgerufen am 13.08.2025)

- Bitwarden
- Enpass Password Manager
- Kaspersky Passwort Manager
- pCloud Pass
- Keeper Passwort-Manager
- LastPass
- mSecure Password Manager
- NordPass
- PassKeep: Passwortmanager
- PassSecurium
- Password Depot
- Password Manager SafeInCloud
- SecureSafe Password-Manger
- Sticky Password Manager+Save
- S-Trust Password Manager

Browserintegrierte Passwortmanager

- Chrome Password Manager
- Mozilla Firefox Password Manager
- Edge Password Manager
- Safari Password Manager
- Opera Password Manager

3.2 Produktauswahl

Die Produktauswahl für die Gefährdungsanalyse erfolgte im 3. Quartal 2024 in mehreren Schritten. Die Auswahl unterteilt sich in zwei browserintegrierte Passwortmanager und acht eigenständige Passwortmanager-Programme.

Um die Wirksamkeit der Untersuchung hinsichtlich der browserintegrierten Passwortmanager sicherzustellen und ein vertretbares Kosten-/Nutzenverhältnis zu gewährleisten, wurden folgende zwei Produkte für die Gefährdungsanalyse ausgewählt:

- Chrome Password Manager
- Mozilla Firefox Password Manager

Diese beiden Browser nehmen anhand der Internetnutzung in Deutschland zwei Drittel des Gesamtmarktes ein.

Von den 19 eigenständigen Passwortmanager-Programmen wurden per Zufallsauswahl die folgenden sechs Produkte für die Gefährdungsanalyse vorausgewählt:

- 1Password (App)
- Avira Password Manager (App)
- mSecurce – Password Manager (App)
- PassSecurium (App)

- S-Trust Passwort-Manager
- SecureSafe Password-Manager

In der zufallsbasierten Vorauswahl wurden keine Keepass-Derivate gezogen. KeePass/kdbx ist ein offenes, nicht-proprietäres Standarddateiformat für Passwortdatenbanken. Wegen der Vielzahl kompatibler Anwendung genießt es hohe Reputation und Verbreitung. Diese Relevanz wird in der qualifizierten Auswahl mitberücksichtigt, daher fand zusätzlich eine qualifizierte Auswahl von zwei Keepass-Derivaten statt. Die folgenden Keepass-Derivate wurden bei der Marktanalyse identifiziert:

- KeePassDroid
- KeePass2Android
- KeepassDX
- JKeePass
- OneKeePass
- KeePassium
- Strongbox
- Strongbox Pro
- Strongbox Zero
- PassDrop 2
- KyPass / Kypass Companion
- KeeWeb
- KeeVault
- KeePassX
- KeePassXC
- MacPass

Unter Berücksichtigung der Kriterien 3 und 4 fiel die Wahl auf KeePassXC als Desktop-Anwendung und KeePass2Android als mobile Anwendung.

4 Grundsätzliche Anforderungen an Passwortmanager

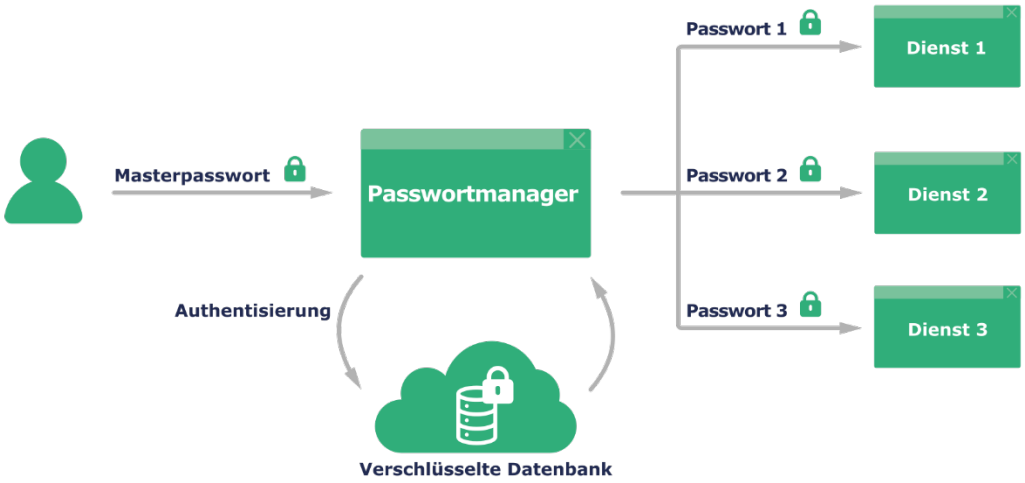

Abbildung 1 Verallgemeinerter Bedienungsablauf eines Passwortmanagers.

Passwortmanager verwalten Passwörter und andere Authentisierungsinformationen, welche Verbraucherinnen und Verbraucher für Onlinedienste verwenden. Mit diesen Daten wird der Zugang zu kritischen, teilweise höchst persönlichen Informationen, wie z.B. dem Onlinebanking, Dating-Profilen oder Gesundheitsinformationen verwaltet. Die Daten müssen daher unbedingt vor dem Zugriff Unbefugter geschützt werden. Zu beachten ist dabei, dass bereits Metainformationen, wie das Wissen, dass eine Person einen Account auf einer Datingplattform hat, kritisch sein können. Aufgrund der Sensibilität der darin gespeicherten Daten, stellen Verbraucherinnen und Verbraucher zurecht höchste Anforderungen an die Sicherheit der von ihnen genutzten Passwortmanager. Wird die Passwortdatenbank an einen Cloud-Speicher ausgelagert, sollten Nutzende sich über den Ort der Speicherung und dessen Schutzniveau informieren[15]. Die wichtigsten Anforderungen sind in 4.1 bis 4.7 enthalten.

4.1 Zugriff nur durch autorisierte Personen

Nur explizit autorisierte Personen dürfen auf die Inhalte des Passwortmanagers zugreifen. Dies bedeutet insbesondere, dass auch Hersteller von Passwortmanagern nicht auf die Daten von Nutzerinnen und Nutzern zugreifen dürfen. Das ist einerseits wichtig, da die Vertrauenswürdigkeit der Hersteller von den Verbraucherinnen und Verbrauchern kaum bewertet werden kann. Andererseits sind Hersteller, die Zugriff auf die Inhalte nehmen können, ein wesentlich attraktiveres Ziel für Cyberangriffe, da Angreifer einfacher an kritischere Daten gelangen können.

[15] Hilfestellung bieten hierbei die verfügbaren Informationen des BSI zur Beachtung bei der Verwendung einer Cloud https://www.bsi.bund.de/dok/130906 (abgerufen am 09.09.2025)

Die Zugriffsmöglichkeiten für Hersteller lassen sich in drei Klassen einteilen:

Zugriffsmöglichkeit	Beschreibung
Kein Zugriff	Der Hersteller kann nicht auf die Inhalte des Passwortmanagers zugreifen.
Bei Benutzung	Der Hersteller kann auf die Inhalte des Passwortmanagers zugreifen, während dieser benutzt wird. Entweder während der regulären Nutzung oder während üblicher Prozesse wie z.B. der Änderung des Masterpassworts. Der Hersteller könnte sich die benötigten Informationen abspeichern und auch im Nachhinein *jederzeit* auf die Inhalte zugreifen.
Jederzeit	Der Hersteller kann jederzeit auf die Inhalte des Passwortmanagers zugreifen. Entweder liegen die Inhalte unverschlüsselt auf den Servern, oder die zur Entschlüsselung benötigten Schlüssel liegen ebenfalls auf den Servern.

Das Vertrauen, das dem Hersteller durch die Verbraucherinnen und Verbraucher entgegengebracht werden muss, sollte auf das absolute Minimum reduziert werden. Das BSI empfiehlt im Kriterienkatalog Cloud Computing[16] für Daten mit einem höheren Schutzbedarf: "Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich und ohne Ausnahme dem Kunden [...] bekannt." (Kapitel 5.8, Eintrag CRY-03). Dies entspricht auch dem Stand der Technik für auf Clouds gespeicherte Daten[17] und wird bei anderen kritischen Daten, wie z.B. in Messengerdiensten (z.B. Signal, Whatsapp, Threema) so umgesetzt und darf von Verbraucherinnen und Verbrauchern so erwartet werden. Eine Zugriffsmöglichkeit durch den Hersteller sollte weder *bei Benutzung* noch *jederzeit* möglich sein. Selbst Metadaten, also Wissen darüber, wann und wie häufig eine Anwendung benutzt wird, können Informationen liefern, die dem Hersteller eine Profilbildung über die Nutzerinnen und Nutzer ermöglichen.

Nutzende sind jedoch immer von der Anwendungssoftware abhängig und Hersteller könnten Hintertüren in neue Softwareversionen einbauen. Daher kann die Anforderung, dass Hersteller gar keinen Zugriff auf die Inhalte des Passwortmanagers haben, streng genommen nicht vollständig erfüllt werden. Dennoch ist es ein wesentlicher Unterschied, ob Server-Administratoren Zugriff nehmen können und die Daten als attraktives Ziel für Cyberangriffe "bereitliegen" oder ob die Sicherheit von der Anwendungssoftware abhängt. Für diese gibt es eine große Bandbreite von Mechanismen, die zusätzlich zur Absicherung der Softwareentwicklung getroffen werden können (z.B. Open Source, regelmäßige Audits, Reproducible Builds[18], Absicherung der Build Pipeline[19]). Die Nutzung dieser Mechanismen erschwert Angreifern das Ausliefern manipulierter Software.

4.2 Transparentes Konzept

Zur Unterstützung unabhängiger Prüfungen sollten Hersteller die von ihnen eingesetzten Konzepte möglichst vollständig öffentlich dokumentieren. Dies beinhaltet insbesondere die Sicherheitskonzepte, die wesentlichen Züge der Systemarchitektur, Details der eingesetzten Kryptographie sowie den Softwareentwicklungsprozess und die darin eingesetzten Schutzmechanismen. Transparent zu zeigen, dass stabile Konzepte eingesetzt werden, ermöglicht detailliertere Prüfungen und erhöht so das Vertrauen von Verbraucherinnen

[16] https://www.bsi.bund.de/dok/409220 (abgerufen am 09.09.2025)

[17] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/,Kapitel 3.2.11 (abgerufen am 09.09.2025)

[18] Bei Reproducible Builds wird garantiert, dass die Kompilierung (das Erzeugen einer ausführbaren Datei aus Quellcode) deterministisch abläuft. Wiederholtes Kompilieren erzeugt also immer wieder dieselbe ausführbare Datei.

[19] Das Absichern der Build Pipeline umfasst alle Maßnahmen, die zum Schutz der im Build-Prozess anfallenden Artefakte ergriffen werden, wie etwa das Setzen entsprechender Berechtigungen für Entwickler nach dem Prinzip der Least Privileges.

und Verbrauchern. Die bloße Nennung kryptographischer Algorithmen ist nicht ausreichend; vielmehr müssen alle relevanten Details, einschließlich Schlüssellängen und Betriebsmodi, offengelegt werden. Besonders Open-Source-Software trägt diesen Anforderungen Rechnung: Wird der Quelltext einer Anwendung öffentlich zugänglich gemacht, erleichtert dies Cybersicherheitsexpertinnen und -experten die Überprüfung des Gesamtkonzepts immens, da die inneren Abläufe einer Anwendung aus dem Quelltext nachvollzogen werden können. Verwendete Bibliotheken sind direkt ersichtlich, Eigenimplementierungen können Instruktion für Instruktion nachvollzogen, Nachbesserungen angemerkt und unabhängige Audits durchgeführt werden. Eine Untersuchung nur auf Basis des Quelltextes ist allerdings extrem aufwändig, daher sollten auch Open-Source-Produkte unbedingt zusätzlich die oben genannten Konzepte veröffentlichen.

4.3 Nutzung etablierter Kryptographie

Die eingesetzte Kryptographie muss auf etablierten Konzepten und Algorithmen sowie unabhängigen Empfehlungen basieren. Die Technische Richtlinie TR-02102-1[20] des BSI enthält eine Bewertung der Sicherheit ausgewählter kryptographischer Verfahren und ermöglicht damit eine längerfristige Orientierung bei der Wahl jeweils geeigneter Methoden. Keinesfalls dürfen selbst erfundene kryptographische Algorithmen eingesetzt werden. Ebenso sollte auf etablierte Implementierungen der genutzten Kryptographie zurückgegriffen und diese keinesfalls selbst implementiert werden.

4.4 Einbindung in das Betriebssystem

Passwortmanager sind immer auch vom zugrundeliegenden Betriebssystem abhängig. Sie sollten daher die vom Betriebssystem angebotenen Funktionen nutzen. Werden diese Funktionen korrekt in der Anwendung eingebunden, unterstützt dies die sichere Benutzung der Anwendenden, z.B. wenn Passwörter auf dem vorgesehenen Weg vom Passwortmanager in den Browser übertragen werden, statt von Nutzenden manuell kopiert und eingefügt zu werden. So kann verhindert werden, dass Passwörter versehentlich an andere Stellen kopiert werden, etwa in einen Chat.

4.5 Bereitstellen von Dokumentation und Erklärungen

Passwortmanager müssen für alle Verbraucherinnen und Verbraucher einfach und sicher zu verwenden sein. Das Bereitstellen einer vollständigen und verständlichen Dokumentation sowie eine gute Nutzerführung im Programm ist unerlässlich. Insbesondere müssen Nutzerinnen und Nutzer sowohl in der Dokumentation, wie auch im täglichen Gebrauch der Passwortmanager über die Folgen ihrer Handlungen, z.B. Änderungen an Konfigurationen, aufgeklärt und ggf. vor möglichen Fehlerquellen gewarnt werden. Dies wird durch eine klare und verständliche Sprache, sichere Standardeinstellungen (Security by default), leicht nachvollziehbare Schritt-für-Schritt-Anleitungen mit visueller Unterstützung, sowie einer Gestaltung der Benutzeroberfläche, die Fehlern vorbeugt und sicherheitsrelevante Funktionen einfach zugänglich macht, erreicht. Transparente Informationen über mögliche Risiken und die getroffenen Schutzmaßnahmen können bei Verbraucherinnen und Verbrauchern einen sicheren Umgang mit Passwortmanagern befördern.

4.6 Sichere Standardkonfiguration

Nach dem Prinzip „Security by default“ müssen Verbraucherinnen und Verbraucher bei der sicheren Nutzung eines Passwortmanagers unterstützt werden. D. h. durch die sichere Standardkonfiguration eines Passwortmanagers sind die Daten von Verbraucherinnen und Verbrauchern von Anfang an optimal geschützt. Hierfür müssen Nutzerinnen und Nutzer zunächst zum Einrichten eines Masterpasswortes angeleitet werden. Sofern Nutzende manuell ein neues Passwort hinterlegen möchten, muss ihnen zum Erstellungszeitpunkt die Qualität des gewählten Passworts angezeigt werden. Zum Schutz der im Passwortmanager gespeicherten Daten sollte standardmäßig eine zeitbasierte Sperrung aktiviert sein, so dass sich dieser nach einem

[20] https://www.bsi.bund.de/dok/433400

Zeitablauf automatisch sperrt. So kann verhindert werden, dass ein Angreifer mit Zugriff auf ein Gerät auch auf die im Passwortmanager gespeicherten Daten Zugriff erhält.

Ebenfalls müssen bei der Cloud-Kommunikation des Passwortmanagers invalide Zertifikate standardmäßig abgelehnt werden. Des Weiteren muss eine Zwei-Faktor-Authentisierung standardmäßig aktiviert sein, da die Angriffsfläche bei der Cloud-Kommunikation wesentlich höher ist als bei der lokalen Speicherung des Passwortmanagers.

Um Angriffe zu verhindern, bei denen ein Angreifer die Kontrolle über eine Subdomäne hat, sollte im Standardfall ein exaktes Domain Matching beim Auto-Fill-Mechanismus eines Passwortmanagers erfolgen.

4.7 Datensicherung und Wiederherstellungsmechanismen

Da in Passwortmanagern sensible Daten gespeichert werden, sollten Hersteller darüber informieren, falls keine automatische Datensicherung existiert. Verbraucherinnen und Verbraucher müssen sich in diesem Fall selbst um die Datensicherung kümmern.

Die in Passwortmanagern abgelegten Passwörter und andere Daten werden verschlüsselt gespeichert. Dies bedeutet, dass der Zugriff nur mit dem Masterpasswort oder mit speziellen Wiederherstellungsmechanismen erfolgen kann. Verbraucherinnen und Verbraucher, die ihr Masterpasswort vergessen, sind von den Wiederherstellungsmechanismen abhängig, um wieder Zugriff auf ihre Daten zu erhalten. Hersteller sollten dies unbedingt unterstützen und Verbraucherinnen und Verbraucher dazu anleiten, einen Wiederherstellungsmechanismus zu aktivieren. Die Funktionsweise von Wiederherstellungsmechanismen ist technisch eng mit der Zugriffsmöglichkeit auf die im Passwortmanager gespeicherten Inhalte verbunden (siehe Unterkapitel 4.1). Es existieren zwei grundlegend verschiedene Konzepte für die Wiederherstellung:

Ohne Zugriffsmöglichkeit des Herstellers:

Der Wiederherstellungsmechanismus basiert darauf, dass Nutzerinnen und Nutzer oder vertrauenswürdige Personen geheime Informationen an einem sicheren Ort ablegen müssen (z.B. in einem Bankschließfach). Wenn das Masterpasswort vergessen wird, kann der Zugriff *nur* mit Hilfe dieser geheimen Informationen wiederhergestellt werden. Der Mechanismus eignet sich auch für die Nutzung als digitaler Nachlass[21] im Todesfall.

Mit Zugriffsmöglichkeit des Herstellers:

Alternativ können Wiederherstellungsmechanismen so gestaltet sein, dass der Hersteller den Zugriff wieder herstellen kann. Ein solcher Mechanismus impliziert, dass der Hersteller Zugriff auf die gespeicherten Inhalte nehmen kann (siehe Unterkapitel 4.1). Ein derart gestalteter Mechanismus sollte unbedingt optional sein und manuell aktiviert werden. Dabei muss die Implikation der Zugriffsmöglichkeit Nutzerinnen und Nutzern unbedingt transparent gemacht werden, sodass diese prüfen können, ob sie dem Hersteller das notwendige Vertrauen entgegenbringen wollen.

[21] In Folge 53 des Podcasts #Updateverfügbar gibt es ein Gespräch mit Johannes Diller vom Digitalen Engel: Das Projekt von Deutschland sicher im Netz e.V. bietet Seniorinnen und Senioren Unterstützung rund um digitale Angebote und stellt auch wertvolle Informationen zum digitalen Nachlass bereit. https://www.bsi.bund.de/dok/1143350 (abgerufen am 22.09.2025)

5 Gefährdungsanalyse

5.1 Methodenbericht

Um eine transparente, nachvollziehbare und vergleichbare Analyse der untersuchten Passwortmanager zu gewährleisten, wurde eine systematische Methodik entwickelt. Diese stützt sich auf ein detailliertes Prüfschema, definierte Testtiefen und realitätsnahe Angreifermodelle. Die folgenden Kapitel erläutern die einzelnen Komponenten dieser Methodik.

5.1.1 Prüfschema

Das zentrale Instrument der Untersuchung ist ein umfassendes Prüfschema. Es dient dazu, die ausgewählten Passwortmanager anhand einer vordefinierten und einheitlichen Liste von Kriterien strukturiert zu beurteilen. Dieses Vorgehen stellt sicher, dass alle untersuchten Produkte unter den gleichen Gesichtspunkten analysiert und die Ergebnisse vergleichbar sind.

Bei der Erstellung des Prüfschemas wurden relevante Aspekte aus anerkannten Standards, Studien und regulatorischen Vorgaben berücksichtigt und übernommen. Die wesentlichen Grundlagen waren die BSI-Studie zu KeePass und Vaultwarden (CAOS 3.0)[22], NIST SP-800-63B-4[23], MITRE ATT&CK®[24], EU Cyber Resilience Act (CRA)[25], BSI TR 03183-01[26], BSI TR-02102-1[27], und OWASP Mobile Application Security Testing Guide (MASTG)[28].

Um eine logische und tiefgehende Analyse zu ermöglichen, ist das Prüfschema in sechs thematische Blöcke gegliedert:

- Basisinformationen
- Verschlüsselung & Kryptographie
- Features
- Synchronisation
- Modellierung und Sicherheitstests
- Prozesse und Vorgehen des Herstellers

Der Fokus des Prüfschemas lag auf der Untersuchung des zugrundeliegenden Konzepts, der eingesetzten kryptographischen Mechanismen sowie der Schnittstellen zu anderen Anwendungen (z. B. Webbrowsern). Die benötigten Informationen wurden dabei aus öffentlichen Quellen, technischen Untersuchungen sowie aus Angaben der Hersteller bzw. Anbieter zusammengetragen.

Das Prüfschema ist in Anhang A: Prüfschema angehängt.

5.1.2 Angreifermodelle

Über die reine Merkmalsprüfung hinaus wurden Angreifermodelle entwickelt, um die Sicherheitsarchitektur der Passwortmanager in einem praxisnahen Kontext zu bewerten. In Anlehnung an das Konzept des "Threat Modeling"[29] verfolgen diese Modelle einen angreiferzentrierten Ansatz. Die Intention war es, die

[22] https://www.bsi.bund.de/dok/1092594 (abgerufen am 18.09.2025)
[23] https://csrc.nist.gov/pubs/sp/800/63/b/4/2pd (abgerufen am 18.09.2025)
[24] https://attack.mitre.org/ (abgerufen am 18.09.2025)
[25] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (abgerufen am 18.09.2025)
[26] https://www.bsi.bund.de/dok/1091552 (abgerufen am 18.09.2025)
[27] https://www.bsi.bund.de/dok/433400 (abgerufen am 18.09.2025)
[28] https://mas.owasp.org/MASTG/ (abgerufen am 18.09.2025)
[29] Ein Prozess, dessen Ziel die Modellierung von Bedrohungen auf schützenswerte Güter ist.

Schutzwirkung der implementierten Sicherheitsfunktionen gegen konkrete, realistische Bedrohungen zu überprüfen.

Die Modelle definieren verschiedene Angreifer mit unterschiedlichen Fähigkeiten und Zugriffsleveln – vom einfachen "Shoulder-Surfing" (Modell A01) über Malware auf dem Endgerät (Modell A05) bis hin zur Kompromittierung des Herstellerservers (Modell A03a). Diese Szenarien ermöglichen eine Bewertung darüber, wie robust ein Passwortmanager gegenüber spezifischen Angriffen ist und welche Gegenmaßnahmen wirksam sind. Die Bedrohungsszenarien, die von diesen Angreifermodellen abgeleitet werden können, nahmen Einzug in den Prüfbogen, um eine bessere Vergleichbarkeit der Resilienz unterschiedlicher Passwortmanager zu ermöglichen.

Die Angreifermodelle sind in Anhang B: Angreifermodelle dokumentiert.

5.1.3 Vorgehen beim Herstellerkontakt

Für viele Prüfpunkte, insbesondere im Bereich interner Prozesse („Prozesse und Vorgehen des Herstellers“), waren die benötigten Informationen nicht öffentlich verfügbar. In diesem Fall wurden konkrete technische Fragen an die jeweiligen Hersteller formuliert und diesen per E-Mail und/oder Brief zugesandt. Einige Hersteller beantworteten die Fragen umfassend. Bei einigen Herstellern gelang die Kontaktaufnahme erst nach Abschluss der Untersuchungen. Alle Hersteller erhielten vom BSI einen ausführlichen Ergebnisbericht zu ihrem untersuchten Produkt, mit der Möglichkeit eine Stellungnahme zu den jeweiligen Prüffeststellungen einzureichen. Die bis zur Erstellung des Abschlussberichtes eingetroffenen Antworten und ggf. im Dialog geklärten offenen Fragen wurden in diesen Bericht einbezogen. Lediglich einer der angefragten Hersteller reagierte weder auf technische Fragen noch auf den übermittelten Ergebnisbericht (Avira Holding GmbH, vgl. Abschnitt 5.2.2).

5.2 Produktspezifische Ergebnisse

Im Folgenden werden die Ergebnisse der Untersuchungen der einzelnen Passwortmanager dargestellt. Tabelle 2 zeigt die zentralen sicherheitstechnischen Eigenschaften und Prüfergebnisse der ausgewählten Passwortmanager zusammengefasst. Danach folgt die Darstellung der Ergebnisse im Detail. Dabei werden die wesentlichen Auffälligkeiten, die für die Beurteilung eines Passwortmanagers relevant sind, aufgeführt. Weitere, weniger relevante Auffälligkeiten wurden den Herstellern in Detailberichten zugesandt und von diesen teilweise bereits behoben.

5.2.1 1Password

Name	1Password
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 8.10.62 für Android, veröffentlicht am 18.02.2025
Hersteller und Sitz des Herstellers	AgileBits Inc., Kanada
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Kein Zugriff
Zentrale Prüffeststellungen	1Password verwendet eine RSA Schlüssellänge von 2048 Bit, was nicht den aktuellen Empfehlungen (siehe BSI TR-02102-1) entspricht. Das Domain-Matching[30] für die Auto-Fill-Funktion ist nicht restriktiv genug eingestellt, um ein versehentliches Übermitteln eines Eintrags an eine manipulierte Adresse zu verhindern.
Herstellerkommunikation	AgileBits reagierte umfassend und detailliert auf den Prüfbericht, wobei darauf verwiesen wurde, dass zukünftige Verbesserungen ständig evaluiert werden würden. Technische Fragen an AgileBits wurden vorab nicht gestellt.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Die Entwickler haben das Sicherheitskonzept mit großer Sorgfalt erstellt, wodurch der Passwortmanager sehr komplex wird. Komplexität birgt allerdings auch das Risiko, dass Schwachstellen übersehen werden könnten. Während der Untersuchung wurden keine Designfehler entdeckt. Insgesamt ergaben sich während der Untersuchung keine grundsätzlichen Bedenken, die gegen die Nutzung von 1Password sprechen.

Tabelle 3 Steckbrief 1Password

[30] Das Auswahlverfahren für verwandte Domains (etwa Subdomains), für die das Passwort ebenfalls gültig sein könnte

5.2.2 Avira Password Manager

Name	Avira Password Manager
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 2.11 für Android, veröffentlicht am 21.03.2025
Hersteller und Sitz des Herstellers	Avira Holding GmbH, Deutschland
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Kein Zugriff
Zentrale Prüffeststellungen	Die eingesetzten kryptographischen Algorithmen konnten nicht überprüft werden. Die biometrische Zugriffskontrolle ermöglicht das Einrichten eines neuen Masterpassworts, ohne das alte zu kennen. Dies birgt insbesondere bei gestohlenen Endgeräten ein Risiko, da der Wiederherstellungsmechanismus auf dieser Funktion basiert.
Herstellerkommunikation	Avira Holding reagierte weder auf technische Fragen, noch auf den Prüfbericht. Avira stellte Informationen zu den eingesetzten kryptographischen Mechanismen, durchgeführten Sicherheitsauditierungen sowie dem Softwareentwicklungsprozess und den eingesetzten zugelieferten Komponenten (Software-Bibliotheken) weder öffentlich noch auf Anfrage zur Verfügung.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Da die kryptographischen Algorithmen nicht geprüft werden konnten, kann dieser wichtige Aspekt nicht bewertet werden. Verbraucherinnen und Verbraucher sollten vor dem Einsatz prüfen, ob sie dem Hersteller ohne objektive Grundlage das notwendige Vertrauen entgegenbringen. Darüber hinaus sollten Nutzende die biometrische Authentifikation in der App deaktivieren und ihr Masterpasswort zusätzlich an einem sicheren Ort aufbewahren, da es keinen anderen Wiederherstellungsmechanismus gibt.

Tabelle 4 Steckbrief Avira Password Manager

5.2.3 Chrome Password Manager

Name	Chrome
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 137.0.7151.69 (Offizieller Build) (64-Bit) unter Windows 10 Pro (22H2), veröffentlicht am 29.04.2025
Hersteller und Sitz des Herstellers	Google, USA
Lizenz	Proprietär, kostenlos
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Zugriffsmöglichkeit ist gegeben bei aktivierter Synchronisation und falls keine Passphrase gesetzt wurde. Es existieren organisatorische Maßnahmen zum Schutz des Schlüsselmaterials.
Zentrale Prüffeststellungen	Chrome ist primär ein Webbrowser, der einen integrierten Passwortmanager aufweist. Die Synchronisation mit dem Google Konto ist optional. Die Zugriffsmöglichkeiten (siehe Unterkapitel 4.1) sind abhängig vom gewählten Modus: • Ohne Synchronisation: kein Zugriff (Standardeinstellung) • Mit Synchronisation im Standardmodus: Jederzeit • Mit Synchronisation mit eigener Passphrase ("Sync Passphrase" Modus[31]): kein Zugriff • Mit Synchronisation im "On-Device-Verschlüsselung" Modus[32]: Bei Benutzung Das Domain-Matching für die Auto-Fill-Funktion ist nicht restriktiv genug eingestellt, um ein versehentliches Übermitteln eines Eintrags an eine manipulierte Adresse zu verhindern.
Herstellerkommunikation	Auf gestellte Fragen im Vorfeld reagierte Google nicht. Im persönlichen Gespräch im Nachgang auf den Prüfbericht wurden Fragen umfassend beantwortet. Der Hersteller verwies zum Synchronisationsmodus auf die Wiederherstellbarkeit des Zugriffs (siehe Unterkapitel 4.7)
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Nutzende sollten bei der Synchronisation über das Google-Konto in den Einstellungen eine eigene Passphrase setzen. Vor der Nutzung eines anderen Modus sollten Verbraucherinnen und Verbraucher prüfen, ob sie dem Hersteller das notwendige Vertrauen entgegenbringen. Wenn sich Nutzende gegen eine Synchronisation über das Google-Konto entscheiden, sollten sie sich unbedingt selbst um Backups der gespeicherten Passwörter kümmern. Weiterhin werden lokal nicht alle Felder verschlüsselt – beispielsweise liegt der Nutzername im Klartext vor. Nutzende sollten daher für sich abschätzen, ob das für sie relevant ist, z.B. weil sie ihr Gerät mit anderen Personen gemeinsam nutzen.

[31] https://support.google.com/chrome/answer/165139
[32] https://support.google.com/accounts/answer/11350823

Tabelle 5 Steckbrief Chrome Password Manager

5.2.4 Keepass2Android

Name	**Keepass2Android**
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 1.12-r5 für Android, veröffentlicht am 22.04.2025
Hersteller und Sitz des Herstellers	Keepass2Android (Open-Source-Projekt), Hauptentwickler Philipp Crocoll, Deutschland
Lizenz	GPL-3 (Open Source)
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Kein Zugriff
Zentrale Prüffeststellungen	Die Keepass2Android-Entwickler betreiben keine eigene Cloud. KeePass2Android nutzt das KeePass 2 (kdbx) Format für den Passwort-Container, das auch von anderen Passwortmanagern, unter anderem dem hier getesteten KeePassXC, unterstützt wird. Keepass2Android bietet keinen Wiederherstellungsmechanismus.
Herstellerkommunikation	Der Entwickler reagierte umfassend auf den Prüfbericht und hat nach eigenen Angaben einige Verbesserungsvorschläge bereits umgesetzt. Technische Fragen wurden an ihn vorab nicht gestellt.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Im Rahmen der Prüftiefe ergaben sich keine Bedenken gegen die Nutzung von Keepass2Android. Nutzende sollten sich bewusst sein, dass sie selbstständig ein Backup erstellen müssen und sich für den Fall des Vergessens des Masterpassworts absichern.

Tabelle 6 Steckbrief Keepass2Android

5.2.5 KeePassXC

Name	**KeePassXC**
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 2.7.9 für Windows, veröffentlicht am 19.06.2024
Hersteller und Sitz des Herstellers	KeePassXC (Open-Source-Projekt)
Lizenz	GPL-2 oder GPL-3 (Open Source)
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Kein Zugriff
Zentrale Prüffeststellungen	Die KeePassXC-Entwickler betreiben keine Cloud. KeePassXC nutzt das KeePass 2 (kdbx) Format für den Passwort-Container, das auch von anderen Passwortmanagern, unter anderem dem hier getesteten Keepass2Android, unterstützt wird. KeePassXC sperrt sich in der Standardeinstellung nicht selbst und bietet keinen Wiederherstellungsmechanismus.
Herstellerkommunikation	Die KeePassXC Entwickler reagierten nicht auf den Prüfbericht, technische Fragen an die Entwickler wurden vorab nicht gestellt.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Im Rahmen der Prüftiefe ergaben sich keine Bedenken gegen die Nutzung von KeePassXC. Verbraucherinnen und Verbraucher sollten sich bewusst sein, dass sie selbstständig ein Backup erstellen müssen und sich für den Fall des Vergessens des Masterpassworts absichern. Falls sie ihr Endgerät teilen oder dieses nicht konsequent gegen unbefugten Zugriff gesichert haben, sollten Verbraucherinnen und Verbraucher die Einstellung aktivieren, dass sich KeePassXC nach einer Zeit selbst sperrt (z.B. 10 Minuten).

Tabelle 7 Steckbrief KeePassXC

5.2.6 Mozilla Firefox Password Manager

Name	**Mozilla Firefox**
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 139.0.1 für Windows, veröffentlicht am 29.05.2025
Hersteller und Sitz des Herstellers	Mozilla Foundation, USA
Lizenz	MPL 2.0
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Kein Zugriff
Zentrale Prüffeststellungen	Firefox ist primär ein Webbrowser, der einen integrierten Passwortmanager aufweist. Die Synchronisation mit dem Mozilla Konto ist optional. Firefox erzwingt standardmäßig nicht das Setzen eines Hauptpassworts, mit welchem die Passwörter lokal verschlüsselt werden und sperrt sich auch nicht selbst.
Herstellerkommunikation	Mozilla reagierte umfassend und detailliert auf den Prüfbericht, technische Fragen an Mozilla wurden vorab nicht gestellt.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Im Rahmen der Prüftiefe ergaben sich keine Bedenken gegen die Nutzung von Firefox. Nutzende sollten in den Einstellungen die Einstellung "Hauptpasswort setzen" aktivieren. Weiterhin sollten Nutzende unbedingt entweder die Synchronisation mit dem Mozilla-Konto aktivieren, oder selbst regelmäßig Backups vornehmen. Nutzende sollten sich für den Fall des Vergessens des Masterpassworts absichern.

Tabelle 8 Steckbrief Firefox Password Manager

5.2.7 mSecure Password Manager

Name	mSecure 6
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 6.1.5 für Android, veröffentlicht am 23.04.2024
Hersteller und Sitz des Herstellers	mSeven Software LLC, USA
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Der Zugriff ist während der Nutzung theoretisch möglich. Der Hersteller gibt an, dass die an den Server gesandte Geheimnisse nicht gespeichert wird.
Zentrale Prüffeststellungen	Es ergaben sich wesentliche Abweichungen von gängigen Empfehlungen. Es werden technische Informationen an den Hersteller gesendet, die es diesem erlauben, auf die Inhalte des Passwortmanagers zuzugreifen. Weiterhin ist es möglich durch die biometrische Zugriffskontrolle ein neues Masterpasswort einzurichten, ohne das alte zu kennen, was ein Risiko insbesondere bei gestohlenen Endgeräten birgt. Der Wiederherstellungsmechanismus basiert auf dieser Funktion. Bei der Implementierung des Passwort-Teilen-Features wird gängige Praxis missachtet und auf ein fragwürdiges Konzept gesetzt, das das Versenden eines Teils des Schlüssels beinhaltet. mSecure verwendet eine RSA Schlüssellänge von 2048 Bit, was nicht den aktuellen Empfehlungen entspricht (siehe BSI TR-02102-1). Informationen zum eingesetzten Konzept, den kryptographischen Mechanismen, durchgeführten Sicherheitsauditierungen sowie dem Softwareentwicklungsprozess und den eingesetzten zugelieferten Komponenten (Software-Bibliotheken) sind nicht öffentlich und transparent verfügbar, wodurch die Durchführung von Sicherheitsuntersuchungen erschwert wird.
Herstellerkommunikation	mSeven Software reagierte nicht auf technische Fragen. Als Reaktion auf den Prüfbericht gab der Hersteller an, die Geheimnisse, welche an ihn übermittelt werden, nicht zu speichern. Außerdem hat der Hersteller das Versenden eines Teils des Schlüssels beim Passwort-Teilen-Feature bestätigt.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Insgesamt erfüllt das Konzept nicht die üblichen Erwartungen an Passwortmanager. Weitere Eigenschaften stützen diese Sicherheitsbedenken. Nutzende sollten vor dem Einsatz prüfen, ob sie dem Hersteller ohne objektive Grundlage das notwendige Vertrauen entgegenbringen.

Tabelle 9 Steckbrief mSecure Password Manager

5.2.8 PassSecurium™

Name	PassSecurium™
Untersuchte Version, Plattform und Veröffentlichungsdatum[33]	Die nachfolgenden Prüffeststellungen beziehen sich ausschließlich auf die Privatkunden-Tarife (FREE/Standard) in den Versionen: Version 1.1.63 (PassSecurium für Android), veröffentlicht am 08.04.2025 Version 2.1.2 (PassSecurium für iOS), veröffentlicht am 10.04.2025 Die Business Instanzen mit kundenverwaltetem Schlüssel waren nicht Gegenstand der Prüfung.
Hersteller und Sitz des Herstellers	ALPEIN Software SWISS AG, Schweiz
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Jederzeit
Zentrale Prüffeststellungen	Der Hersteller ist technisch dazu in der Lage, jederzeit auf die gespeicherten Inhalte zuzugreifen (siehe Unterkapitel 4.1), da die dazu notwendigen Schlüssel auf den Servern vorliegen. Es wurden Schwächen in der Implementierung der genutzten Kryptographie sowie nicht empfohlene Algorithmen identifiziert. In der App ist es möglich, das Masterpasswort mit Kenntnis des minimal 5-stelligen Sicherheitscodes im Klartext anzuzeigen.
Herstellerkommunikation	ALPEIN Software SWISS reagierte im Vorfeld auf technische Fragen. In der schriftlichen Antwort und im persönlichen Gespräch, die auf den Prüfbericht folgten, verwies der Hersteller auf ein großes Update, das zeitnah folgen und die Defizite adressieren solle.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Die Tatsache, dass der Hersteller *jederzeit* auf gespeicherte Passwörter von Nutzenden zugreifen kann, ist mit grundsätzlichen Sicherheitsanforderungen an Passwortmanager unvereinbar. Bis zum Rollout des Master-Upgrades (Version 3.x) wird von der Nutzung der getesteten Apps (Android 1.1.63 / iOS 2.1.2) in den Tarifen FREE/Standard abgeraten. Der Hersteller empfiehlt, auf die jeweils aktuellen Versionen zu aktualisieren, sobald diese verfügbar sind.

Tabelle 10 Steckbrief PassSecurium™

[33] Die Feststellungen beziehen sich auf den Entwicklungsstand vor dem Master-Upgrade (Version 3.x).“

5.2.9 SecureSafe Password-Manager

Name	SecureSafe
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 2.24.1 für Windows, veröffentlicht am 20.11.2024
Hersteller und Sitz des Herstellers	DSwiss AG, Schweiz
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Der Zugriff ist während der Nutzung theoretisch möglich. Der Hersteller gibt an, dass die Schlüssel während einer aktiven Sitzung nur im Hauptspeicher des Servers vorliegen.
Zentrale Prüffeststellungen	Das zugrundeliegende kryptographische Konzept basiert auf einem serverseitigen Ver- und Entschlüsseln der Inhalte (siehe Unterkapitel 4.1). Dies erhöht prinzipiell die Angriffsfläche auf Seiten des Herstellers, die durch kompensatorische Maßnahmen mitigiert werden muss. Nutzende müssen diesen zusätzlich ergriffenen Maßnahmen vertrauen. Das Domain-Matching für die Auto-Fill-Funktion ist nicht restriktiv genug eingestellt, um ein versehentliches Übermitteln eines Eintrags an eine manipulierte Adresse zu verhindern. Informationen zum eingesetzten Konzept, den kryptographischen Mechanismen, durchgeführten Sicherheitsauditierungen sowie dem Softwareentwicklungsprozess und den eingesetzten zugelieferten Komponenten (Software-Bibliotheken) sind nicht öffentlich und transparent verfügbar, was die Durchführung von Sicherheitsuntersuchungen erschwert.
Herstellerkommunikation	Nach Übermittlung des Prüfberichtes und im Zeitraum bis zur Veröffentlichung des Abschlussberichtes nahm DSwiss Stellung und beantwortete die vor der Untersuchung gestellten Fragen.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Das Produkt SecureSafe in der untersuchten Version 2.24.1 basiert auf der serverseitigen Ver- und Entschlüsselung von Inhalten. Der Hersteller gab an, dass die theoretische Möglichkeit eines Zugriffs durch kompensatorische Maßnahmen unterbunden wird. Diese waren nicht Bestandteil der Untersuchung. Verbraucherinnen und Verbraucher sollten vor dem Einsatz immer prüfen, ob sie den kompensatorischen Maßnahmen des Herstellers vertrauen. Diese sind abrufbar unter: https://www.dswiss.com/de/solutions/security.

Tabelle 11 Steckbrief SecureSafe Password-Manager

5.2.10 S-Trust Password Manager

Name	S-Trust
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 4.0.1 für Windows, veröffentlicht am 20.12.2024
Hersteller und Sitz des Herstellers	S-Communication Services GmbH
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller (siehe Unterkapitel 4.1)	Da es sich bei S-Trust technisch um SecureSafe der DSwiss AG handelt (White-Label-Produkt), gelten hier die gleichen Zugriffsmöglichkeiten.
Zentrale Prüffeststellungen	Da es sich bei S-Trust technisch um SecureSafe der DSwiss AG handelt (White-Label-Produkt), gelten hier die gleichen zentralen Prüffeststellungen.
Herstellerkommunikation	Die S-Communication Services GmbH reagierte auf technische Fragen im Vorfeld und beantwortete sie ausführlich. In Bezug auf die im anschließenden Prüfbericht genannten Rückfragen verwies der Anbieter auf die DSwiss AG als Entwickler. Die S-Communication Services GmbH gab an, dass der Produktbetrieb von S-Trust Password Manager spätestens zum 31. März 2026 eingestellt wird.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Da es sich bei S-Trust technisch um SecureSafe der DSwiss AG handelt (White-Label-Produkt), gelten hier die gleichen Einschätzungen und Empfehlungen für Verbraucherinnen und Verbraucher.

Tabelle 12 Steckbrief S-Trust Password Manager

6 Schlussfolgerungen und Handlungsempfehlungen

Im Folgenden werden Maßnahmenempfehlungen für Hersteller sowie Verbraucher und Verbraucherinnen vorgestellt, die einen sicheren Betrieb der Passwortmanager gewährleisten sollen. Bei der Auswahl eines geeigneten Produkts kommt es vor allem auf die Verfügbarkeit einer technischen Dokumentation an. Viele der untersuchten Produkte präsentieren sich mit reinen Marketing-Versprechen, ohne die eingesetzte Architektur oder die eingesetzten Mechanismen im Hintergrund zu beleuchten. Auch wenn Laien den Ausführungen nicht gänzlich folgen können, bedeutet das Fehlen öffentlicher technischer Dokumentation und Whitepaper, dass das Produkt unter erschwerten Bedingungen extern geprüft werden kann. Eine öffentliche Dokumentation von Audit-Berichten und Ergebnissen von technischen Penetrationstests ist ein guter Hinweis darauf, dass der Hersteller hohes Vertrauen in sein Produkt hat und transparent mit Problemen umgeht. Grundsätzlich begrüßenswert sind in dieser Hinsicht Open Source-Produkte, da durch das Verfügbarmachen von Quellcode zusätzlich Transparenz geschaffen wird: Interessierte können einen direkten Blick in die innere Wirkungsweise der Software nehmen und sich von der korrekten Umsetzung überzeugen.

6.1 Empfehlungen für Hersteller/Anbieter

Die hier vorgestellten Empfehlungen erweitern die Liste der unter Kapitel 4 aufgezählten grundlegenden Anforderungen.

Transparenz ist ein Schlüsselaspekt für sichere Software. Hersteller sollten ihren Software-Entwicklungsprozess, die verwendeten Drittparteibibliotheken sowie die Information zu durchgeführten Sicherheitsaudits und Penetrationstests veröffentlichen. Dies hilft nicht nur dabei das Vertrauen der Endkunden zu stärken, sondern ermöglicht es auch, schnell auf potenzielle Schwachstellen zu reagieren.

Die Verwendung eines Auto-Fill-Dienstes trägt dazu bei, dass Verbraucherinnen und Verbraucher ihre Passwörter nicht in die Zwischenablage kopieren und somit ungewollt an falscher Stelle einfügen könnten. Zusätzlich sollten sensible Inhalte vor dem Anfertigen von Bildschirmfotos geschützt, alle Daten, einschließlich Metadaten, verschlüsselt, und die Anwendungen (Apps) mit digitalen Signaturen vor Fälschungen geschützt werden.

Während der Passworterstellung sollten Nutzende Indikatoren für die Passwortstärke erhalten, die sich an Empfehlungen wie z.B. denen der NIST[34] orientieren. Es sollte eine Standardzeitüberschreitung (Time-out) geben, nach der der Passwortmanager gesperrt wird und die Verwendung eines Masterpassworts sollte standardmäßig voreingestellt sein.

Ein weiterer wichtiger Punkt ist die Schreibkonfliktbewältigung bei der Synchronisation über eine Cloud. Verfolgt ein Passwortmanager einen strikten Least-Recently-Used-Ansatz, bei dem Änderungen mit einem neueren Zeitstempel vorangegangene Änderungen einfach überschreiben, kann dies zu Datenverlust bei den Verbraucherinnen und Verbrauchern führen, sofern diese mit mehreren Endgeräten gleichzeitig auf dieselbe Datenbank zugreifen. Hersteller sollten die Verbraucherinnen und Verbraucher daher warnen, sofern Passworteinträge überschrieben werden würden.

Die Entwicklung von Passwortmanagern ist inhärent kompliziert und fehleranfällig. Unternehmen, die ihren Kundinnen und Kunden einen Passwortmanager anbieten möchten, sollten prüfen, ob sie diesen selbst entwickeln wollen oder ob es sinnvoller ist, einen etablierten Passwortmanager als White-Label-Produkt zuzukaufen und unter eigener Marke bereitzustellen. Um das Vertrauen der Nutzenden nicht zu missbrauchen, sollten Hersteller die hier aufgeführten Empfehlungen beherzigen und das dem Passwortmanager zugrundeliegende Konzept regelmäßig evaluieren. Hilfreich ist, die Passwortmanager in einer bereits sicheren Standardeinstellung auszuliefern, die Felder der Einträge vollständig zu verschlüsseln, um keine Metainformationen preiszugeben und bei sicherheitsrelevanten Änderungen Hinweise anzuzeigen. Außerdem sollten Verbraucherinnen und Verbraucher auf die Notwendigkeit von Backups hingewiesen werden.

[34] https://csrc.nist.gov/pubs/sp/800/63/b/4/2pd (abgerufen am 18.09.2025)

Nach Änderungen am Masterpasswort sollten die Passwort-Container immer neu verschlüsselt werden, um potenzielle Angriffsvektoren auszuschließen. Asymmetrische Verschlüsselung sollte für das Teilen sensibler Daten verwendet werden. Es ist auch ratsam, dass Nutzende beim Ändern ihres Masterpassworts auf einem bereits entsperrten Gerät erneut nach ihrem Passwort gefragt werden, um Angriffe zu erschweren.

Der Einsatz von Zertifikat-Pinning[35] trägt dazu bei, Machine-in-the-Middle-Angriffe und gefälschte Zertifikate zu verhindern. Allgemein sollte standardmäßig nicht allen Zertifikaten getraut werden: Invalide Zertifikate sollten grundsätzlich abgelehnt werden.

6.2 Empfehlungen für Verbraucherinnen und Verbraucher

Zunächst sollten sich Verbraucherinnen und Verbraucher vor der Auswahl eines Passwortmanagers gründlich über die Funktionalitäten und Sicherheitsmerkmale ihrer präferierten Anwendung informieren, um sicherzustellen, dass ihre Passwörter und sensiblen Daten adäquat geschützt sind.

Die Auswahl und Einrichtung eines Masterpassworts sind von entscheidender Bedeutung für die Sicherheit der zu speichernden Inhalte. Wenn die Verwendung eines Masterpassworts nicht standardmäßig aktiviert ist, sollten Verbraucherinnen und Verbraucher dies umgehend ändern, um zu gewährleisten, dass andere Personen, die das gleiche Endgerät verwenden, nicht auf die Geheimnisse zugreifen können.

Ein weiterer wichtiger Aspekt ist die Fähigkeit eines Passwortmanagers, automatisierte Backups zu erstellen. Sollten Backups vom Passwortmanager nicht automatisch erstellt werden, müssen Nutzende selbst für das Erstellen von manuellen Backups sorgen, indem sie für sich ein Backup-Konzept erarbeiten und umsetzen.

Bei Funktionalitäten, die versprechen im Notfall eine Hintertür für Verbraucherinnen und Verbraucher selbst oder Angehörige zu bieten, sollte näher recherchiert werden. Solch ein Notfallzugriff muss vernünftig und sicher implementiert sein, um keinen zusätzlichen Angriffsvektor zu bieten. Müssen für den Notfallzugriff *vorab* Zugriffsinformationen abgespeichert werden, die nicht verloren gehen dürfen, lässt dies auf ein stabileres Konzept schließen. Bei Mechanismen, bei denen der Hersteller den Zugriff erst im Nachgang erstellen kann, sollte genau geprüft werden, ob dem Hersteller das notwendige Vertrauen entgegen gebracht werden kann (siehe Unterkapitel 4.7).

Die Einrichtung der automatischen Sperrung ist ein weiteres wichtiges Sicherheitsmerkmal, das Nutzende überprüfen sollten. Manche Passwortmanager sperren den Zugriff auf die Geheimnisse nicht standardmäßig nach einer gewissen Zeit, was bedeutet, dass Verbraucherinnen und Verbraucher den Passwortmanager nach der Verwendung gegebenenfalls selbst sperren müssen, um anderen Personen, die das Endgerät ebenfalls nutzen, keinen Zugriff auf Geheimnisse zu gewähren.

Darüber hinaus sollten Verbraucherinnen und Verbraucher, wo immer es möglich ist, die Zwei-Faktor-Authentisierung (2FA) aktivieren. Dabei sollten in erster Linie Hardware-Tokens in Erwägung gezogen und der Einsatz von TOTPs (Time-Based One-Time Passwords[36]) evaluiert werden. Auf SMS-OTP-Varianten sollte verzichtet werden, sofern es andere 2FA-Möglichkeiten gibt, da diese anfälliger für bestimmte Angriffe, wie etwa SIM-Swapping[37], sind.

Insgesamt gibt es eine große Auswahl an Produkten mit unterschiedlichen Vor- und Nachteilen. Die in Absatz 4 aufgeführten Anforderungen bieten eine Übersicht, welche Eigenschaften Verbraucherinnen und Verbraucher bei der Auswahl eines Passwortmanagers beachten sollten. Leider sind viele entscheidende technische Details, wie z.B. der Einsatz angemessener Verschlüsselungsverfahren oder die zugrundeliegenden Konzepte nur mit viel Aufwand und Sachverstand prüfbar. Die Eigenschaften der im Rahmen dieses

[35] Digitale Zertifikate werden dafür genutzt, Kommunikationspartner zu authentisieren, d.h. ihre Echtheit zu prüfen. Vergleichbar zur Akzeptanz von Ausweisdokumenten in der analogen Welt, dürfen nur valide Zertifikate akzeptiert werden. Zertifikat-Pinning erhöht die Sicherheit zusätzlich.

[36] verbreiteter Zweiter-Faktor-Mechanismus, bei dem ein sechsstelliger Code generiert wird, der durch die Nutzenden abgetippt werden muss.

[37] Ein Angriff, bei dem Angreifende es schaffen, beim Mobilfunkanbieter eine zweite SIM-Karte zur selben Rufnummer zu erhalten. So können z.B. SMS Nachrichten abgefangen werden.

Projektes untersuchten Passwortmanager sind in *Tabelle 2* übersichtlich dargestellt. Zusätzlich können Verbraucherinnen und Verbraucher auf unabhängige Tests seriöser Organisationen und Medien zurückgreifen.

7 Anhang

7.1 Prüfschema

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
	Basisinformationen			
1	Name	Basisinformation	Freitext	Webseite / Recherche
2	Untersuchte Version, Plattform und Veröffentlichungsdatum	Basisinformation	Freitext	Webseite / Recherche
3	Hersteller	Basisinformation	Freitext	Webseite / Recherche
4	Eigenbeschreibung des Programms	Basisinformation	Freitext	Webseite / Recherche
5	Sitz des Herstellers	Basisinformation	Freitext	Webseite / Recherche
6	Lizenz	Basisinformation	Freitext	Webseite / Recherche
7	Erstveröffentlichung	Basisinformation, gibt Auskunft über Marktreife	Datum	Webseite / Recherche
8	Datum des letzten Updates	Wichtiger Indikator für Wartung und Sicherheitsupdates	Datum	Webseite / Recherche
9	Entsprechen die dem Produkt beigefügten Informationen den Anforderungen des CRA Anhang II sowie BSI TR 03183-01 REQ_UD 1 - REQ_UD 6?	Compliance zum CRA Compliance zu BSI TR 03183-01	Jeweils: „Ja“ / „Nein“ / Freitext zu Abweichungen Zu den folgenden Punkten: • CRA Anhang II Nr. 1 • CRA Anhang II Nr. 2 • CRA Anhang II Nr. 3 • CRA Anhang II Nr. 4 • CRA Anhang II Nr. 5 • CRA Anhang II Nr. 6 • CRA Anhang II Nr. 7 • CRA Anhang II Nr. 8 a) • CRA Anhang II Nr. 8 b) • CRA Anhang II Nr. 8 c)	Webseite / Recherche

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
			• CRA Anhang II Nr. 8 d) • CRA Anhang II Nr. 8 e) • CRA Anhang II Nr. 8 f) • CRA Anhang II Nr. 9 • BSI TR 03183-01 REQ_UD 1 • BSI TR 03183-01 REQ_UD 2 • BSI TR 03183-01 REQ_UD 3.1 • BSI TR 03183-01 REQ_UD 3.2 • BSI TR 03183-01 REQ_UD 4 • BSI TR 03183-01 REQ_UD 5 • BSI TR 03183-01 REQ_UD 6	
	Verschlüsselung & Kryptographie			
10	Bei der Auswahl des Master-Passworts: Gibt es Indikatoren für die Qualität des Passworts?	NIST SP-800-63B-4 2pd	Ja / Nein	Einfacher Test der Anwendung
11	Welcher Algorithmus wird für die Bewertung der Qualität des Master-Passworts verwendet?	NIST SP-800-63B-4 2pd	Freitext	Dokumentation, Herstellerfeedback, erweiterter Test der Anwendung
12	Entsprechen die Indikatoren für die Bewertung der Qualität des Master-Passworts den Empfehlungen der NIST?	Schlechte Güteindikatoren bringen keinen Mehrwert oder führen zu schlechteren Passwörtern. NIST SP-800-63B-4 2pd	Ja / Nein / n.a.	Dokumentation, Herstellerfeedback, erweiterter Test der Anwendung
13	Gibt es Vorgaben für die Qualität des Master-Passworts?	NIST SP-800-63B-4 2pd	Ja / Nein	Einfacher Test der Anwendung
14	Kann das Master-Passwort geändert werden?	Nutzbarkeit, Prüfung auf konzeptionelle Schwächen	Ja / Nein	Einfacher Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
15	Können nach Änderung des Master-Passworts weiterhin mit dem alten Passwort Informationen aus dem neuen Container abgeleitet werden?	Prüfung auf konzeptionelle Schwächen	Ja / Nein	Dokumentation, Herstellerfeedback, erweiterter Test der Anwendung (z.B. mit einem Hex-Editor)
16	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Prozesses zur Änderung des Master-Passworts?	Prüfung auf konzeptionelle Schwächen	Ja, Freitext / Nein	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung
17	Kann eine zwei-Faktor-Authentisierung zum Entsperren des Passwortmanagers genutzt werden?	Sicherheit & Vertrauen MITRE Credential Access TA0006 T1111 (Multi-Factor Authentication Interception)	Ja / Nein	Dokumentation, einfacher Test der Anwendung
18	Kann der Passwortmanager durch andere Mechanismen als das Master-Passwort entsperrt werden?	Prüfung auf konzeptionelle Schwächen	Ja / Nein	Dokumentation, einfacher Test der Anwendung
19	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse der Zwei-Faktor-Authentisierung zum Entsperren des Passwortmanagers?	Sicherheit & Vertrauen MITRE Credential Access TA0006 T1111 (Multi-Factor Authentication Interception)	Ja, Freitext / Nein	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung
20	Gibt es eine Recovery-Option bei Verlust des Master-Passworts?	Prüfung auf konzeptionelle Schwächen MITRE Credential Access TA0006 T1621 (Multi-Factor Authentication Request Generation)	Ja / Nein	Dokumentation, Herstellerfeedback, einfacher Test der Anwendung
21	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Prozesses zum Recovery des Master-Passworts?	Prüfung auf konzeptionelle Schwächen MITRE Credential Access TA0006 T1621 (Multi-Factor Authentication Request Generation)	Ja, Freitext / Nein	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
22	Welche kryptografischen Algorithmen werden verwendet und sind diese in ihrer Verwendung konform mit BSI TR-02102-1?	Konformität mit BSI TR 02102-1	Tabelle über: Funktion, Algorithmus, TR-02102-1 compliant	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
23	Sind alle eingesetzten kryptographischen Algorithmen resistent gegen Brute-Force-Angriffe?	MITRE Credential Access TA0006 T1110 (Brute Force) • MASTG-TEST-0208	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
24	Erfolgt die Verschlüsselung mit einem Post-Quanten-Kryptographie Algorithmus?	Sicherheit gegen zukünftige Angriffe Konformität mit BSI TR 02102-1	Ja / Nein	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
25	Wird selbst implementierte Kryptografie genutzt?	Prüfung auf konzeptionelle Schwächen • MASTG-TEST-0221	Ja / Nein	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
26	Wird der komplette Inhalt vollständig verschlüsselt? • Passwörter • Benutzernamen • URLs • Favicons • Dateien	Prüfung auf konzeptionelle Schwächen	Ja / Nein	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
	Features			
27	Gibt es einen Passwortgenerator?	Unterstützt bei der Wahl von sicheren Passwörtern	Ja / Nein	Einfacher Test der Anwendung
28	Welcher Algorithmus wird für die Bewertung der Qualität von gespeicherten Passwörtern verwendet?	NIST SP-800-63B-4 2pd	Freitext	Dokumentation, Herstellerfeedback, erweiterter Test der Anwendung
29	Entsprechen die Indikatoren für die Bewertung der Qualität von	NIST SP-800-63B-4 2pd	Ja / Nein / n.a.	Dokumentation, Herstellerfeedback, erweiterter Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
	Passwörtern den Empfehlungen der NIST?			
30	Gibt es die Möglichkeit, Daten zum Ausfüllen von Authentisierungsinformationen an andere Programme zu übertragen (Browser, Apps)?	Nutzungskomfort, sowie Sicherheit gegen Fehlbedienung	Ja / Nein	Dokumentation, einfacher Test der Anwendung
31	Mit welchen gängigen Browsern ist der Passwortmanager kompatibel?	Reichweite und Kompatibilität	Freitext	Dokumentation, einfacher Test der Anwendung
32	Wird Host, Domain oder Subdomain gematcht?	Relevanz für Sicherheit (Phishing) MITRE Credential Access TA0006 T1557.004 (Adversary-in-the-Middle / Evil Twin) Aus CAOS: • Unsicheres globales Auto-Type-Feature	Freitext	Erweiterter Test der Anwendung
33	Werden Nutzername und Passwort beim Laden der Website automatisch ausgefüllt oder braucht es Nutzerinteraktionen?	Automatisierungsgrad der Anwendung, Sicherheit MITRE Credential Access TA0006 T1187 (Forced Authentication) Aus CAOS: Unsicheres globales Auto-Type-Feature	Freitext	Einfacher Test der Anwendung
34	Wird eine Warnung angezeigt, wenn Nutzende im Browser ein Passwort zum Einfügen auswählen, bei dem die hinterlegte URL auf Domain Ebene nicht zur aktuellen Webseite passt?	Relevanz für Sicherheit (Phishing) Nutzungskomfort, sowie Sicherheit gegen Fehlbedienung	Ja / Nein	Einfacher Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
35	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse der Verbindung des Passwortmanagers mit dem Browser sowie dem Matching der Webseite im Browser?	Prüfung auf konzeptionelle Schwächen Aus CAOS: • Unsicheres globales Auto-Type-Feature • Passwörter potenziell in der URL übertragen • Folgen von Weiterleitung beim Öffnen entfernter Datenbanken	Ja, Freitext / Nein	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung
36	Welche Sicherheitsmechanismen des Betriebssystems werden verwendet (z.B. TPM, Lockscreen Trigger)? Wie werden diese jeweils verwendet?	Prüfung auf konzeptionelle Schwächen	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
37	Wird die Zwischenablage automatisch geleert, wenn die vom PWM vorgesehene Funktion zum Kopieren verwendet wird? Wenn ja, nach welcher Zeit?	Schutz vor unbefugtem Zugriff MITRE Credential Access TA0006 T1003 (OS Credential Dumping)	Ja / Nein / n.a.	Einfacher Test der Anwendung
38	Sperrt sich der PWM automatisch nach einer gewissen Zeit? Wenn ja, nach welcher Zeit?	Schutz vor unbefugtem Zugriff	Ja / Nein	Einfacher Test der Anwendung
39	Gibt es eine Funktion zum Export von Passwörtern?	Nutzerkontrolle über Daten, Kompatibilität	Ja / Nein	Einfacher Test der Anwendung
40	In welche verschlüsselten und unverschlüsselten Formate kann exportiert werden?	Kritisch für Sicherheit beim Datenexport Aus CAOS 3.0: Ein Angreifer kann über Export-Trigger Klartext-Passwörter extrahieren.	Freitext	Einfacher Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
41	Gibt es eine Funktion zum sicheren Teilen von Passwörtern mit anderen Personen oder Instanzen?	Flexibilität und Nutzungsszenarien	Ja / Nein	Einfacher Test der Anwendung
42	Wie ist die Funktion zum Teilen von Passwörtern mit anderen Personen oder Instanzen umgesetzt?	Flexibilität und Nutzungsszenarien	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
43	Gibt es eine Funktion, um Passwörter gegen bekannte Leaks zu prüfen? (z. B. "*Have I Been Pwned*"?)	Information bei bekannten kompromittierten Passwörtern, ermöglicht Nutzenden zeitnah die Passwörter beim jeweiligen Dienst zu ändern	Ja / Nein	Einfacher Test der Anwendung
44	Läuft diese Prüfung automatisch?	Effizienz und Schutz	• Ja, aber deaktivierbar • Ja, aber nicht deaktivierbar • Nein, aber aktivierbar • Nein, aber manuell • Nein • n.a.	Einfacher Test der Anwendung
45	Unterstützt der Passwortmanager die Verwaltung von zusätzlichen Authentisierungsfaktoren für Zwei-Faktor-Authentisierung bei anderen Diensten (z.B. TOTP)?	Relevantes Feature, die Verortung von zwei Faktoren in einer Komponente könnte der Idee von Zwei-Faktor Authentisierung widersprechen. Die Erhebung ermöglicht eine Auswertung und Diskussion des Features. MITRE Credential Access TA0006 T1111 (Multi-Factor Authentication Interception)	Ja, Liste / Nein	Dokumentation, einfacher Test der Anwendung
	Synchronisation			
46	Können gespeicherte Daten über eine Cloud synchronisiert werden?	Datenschutz, Datenhoheit, Funktionalität	Ja / Nein	Einfacher Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
47	Können Nutzende den Speicherort für die Online-Synchronisation frei wählen, welche stehen zur Auswahl?	Datenschutz, Datenhoheit	Ja / Nein + Freitext	Dokumentation, einfacher Test der Anwendung
48	Betreibt der Hersteller einen angebotenen Speicherort selbst? Falls nein: Welche Anbieter nutzt er?	Datenschutz, Datenhoheit	Freitext	Dokumentation, Herstellerfeedback
49	In welchem Land werden Daten gespeichert?	Datenschutzvorgaben können variieren (z. B. DSGVO)	Freitext	Dokumentation, Herstellerfeedback
50	Wie authentisieren sich Nutzende gegenüber dem vom Hersteller angebotenen Speicherort?	Prüfung auf konzeptionelle Schwächen	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
51	Werden Maßnahmen eingesetzt, um Brute-Force-Angriffe zu unterbinden und wie sind diese umgesetzt?	MITRE Credential Access TA0006 T1110 (Brute Force)	Freitext	Dokumentation, Herstellerfeedback
52	Wird Transportverschlüsselung und Zertifikat-Pinning korrekt umgesetzt?	Schutz gegen machine-in-the-middle Angriffe Aus CAOS 3.0: Fehlerhafte Zertifikatsüberprüfung • MASTG-TEST-0206 • MASVS-NETWORK: 0218, 0235, 0236,	Ja / Nein	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
53	Was wird synchronisiert: Container oder Einzelobjekte?	Schutz gegen Auswertung von Metadaten durch die Betreibenden des Speicherorts, Schutz gegen Malware Angriffe	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung
54	Wie werden Konflikte bei der Synchronisation gelöst?	Sicherstellen der Datenintegrität	Freitext	Dokumentation, Herstellerfeedback, komplexer Test der Anwendung

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
55	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Synchronisationsmechanismus? Welche Informationen kann der Hersteller, beziehungsweise der Serverbetreiber lernen?	Prüfung auf konzeptionelle Schwächen	Ja, Freitext / Nein	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung
	Modellierung und Sicherheitstests			
56	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Passwortmanagers?	Prüfung auf konzeptionelle Schwächen MITRE Credential Access TA0006 T1212 (Exploitation for Credential Access)	Freitext	Modellierung, auf Basis von Dokumentation, Herstellerfeedback oder komplexem Test der Anwendung
57	Für Android-Apps: Werden alle Tests der OWASP MASVS-RESILIENCE-Klasse erfüllt?	MASTG-TEST-0224, 0225, 0226, 0227[2] (2): Nur testbar durch Dekompilieren.	Ja / Nein	Komplexer Test der Anwendung (statische Analyse)
58	Für Android-Apps: Können sensitive Daten durch andere Apps gelesen werden?	MASVS-STORAGE: 0200, 0201, 0203, 0207, 0216	Ja / Nein	Komplexer Test der Anwendung (dynamische Analyse)
	Prozesse und Vorgehen des Herstellers			
59	Wurden bereits Sicherheits-Audits für dieses Produkt durchgeführt?	Indikator zur Marktreife und Ausgereiftheit	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche
60	Wer hat die Sicherheits-Audits beauftragt?	Prüfung auf potenzielle Interessenskonflikte	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche
61	Wurden bereits Penetrationstests für dieses Produkt durchgeführt?	Indikator zur Marktreife und Ausgereiftheit MITRE Credential Access TA0006 T1212 (Exploitation for Credential Access)	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche
62	Wer hat diese Penetrationstests beauftragt?	Prüfung auf potenzielle Interessenskonflikte	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche

	Eintrag	Begründung und/oder Prüfgrundlage	Ergebnis Form	Quelle & Vorgehen
63	Gab es bereits erfolgreiche Angriffe auf den Passwortmanager?	Indikator zur Marktreife und Ausgereiftheit	Ja / Nein	Dokumentation, Herstellerfeedback, Internetrecherche
64	Falls ja: Wie reagierte der Hersteller auf den Angriff?	Ein unprofessioneller Umgang ist ein Indikator dafür, dass der Hersteller zukünftig auch nicht professionell reagieren könnte. Compliance zu CRA / BSI TR-03183-3	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche
65	Wie reagiert der Hersteller auf Schwachstellen?	Ein unprofessioneller Umgang ist ein Indikator dafür, dass der Hersteller zukünftig auch nicht professionell reagieren könnte. Compliance zu CRA / BSI TR-03183-3	Freitext	Dokumentation, Herstellerfeedback, Internetrecherche
66	Werden öffentlich Informationen zu Sicherheitsaktualisierungen bereitgestellt?	Einblick in Verantwortungsbewusstsein des Herstellers bezüglich Updates Compliance zum CRA Anhang I Teil II Nr. 4	Ja, Einschätzung zu Compliance /Nein, Erklärung ob Hinweise auf bereits geschlossene Sicherheitslücken existieren.	Dokumentation, Herstellerfeedback
67	Existiert ein sicherer Updatekanal?	Compliance zum CRA Anhang I Teil II Nr. 7 Compliance zu BSI TR 03183-01 REQ_VH 6	Ja, Einschätzung zu Compliance / Nein	Dokumentation, Herstellerfeedback
68	Existiert ein öffentlich dokumentiertes Konzept für die koordinierte Offenlegung von Schwachstellen sowie ein Kontaktpunkt dazu?	Compliance zum CRA Anhang I Teil II Nr. 5 & 6 Compliance zu BSI TR 03183-01 REQ_VH 5 Compliance zu BSI TR 03183-03	Ja, Einschätzung zu Compliance, Verweis / Nein	Dokumentation, Herstellerfeedback

Tabelle 13 Prüfschema für den einheitlichen Vergleich der untersuchten Passwortmanager

7.2 Definitionen

Art des Tests	Definition
Einfacher Test	Der Test kann nach derzeitiger Einschätzung mit hoher Wahrscheinlichkeit durchgeführt werden und ein Ergebnis liefern.
Erweiterter Test	Der Test kann nach derzeitiger Einschätzung mit mittlerer Wahrscheinlichkeit durchgeführt werden und ein Ergebnis liefern.
Komplexer Test	Es ist derzeit unklar, ob der Test durchgeführt werden ein Ergebnis liefern kann.

Tabelle 14 Definitionen der verwendeten Testarten

7.3 Angreifermodelle

7.3.1 A01: Angreifer hat Zugriff auf das Masterpasswort (z. B. Post-it, Shoulder-Surfing)

- Erläuterung

Angreifer A01 kennt das Masterpasswort, das zum Entschlüsseln des Passwortmanagers genutzt wird, sowie den Hersteller des Passwortmanagers und ggf. den Nutzernamen. Er hat jedoch insbesondere keinen Zugriff auf die Container-Datei.

- Beispielszenario

Eine Nutzerin nutzt ihren Passwortmanager im Zug und bemerkt nicht, dass ihre Sitznachbarin sowohl den Hersteller des Passwortmanagers, wie auch den Nutzernamen mitliest und durch *Shoulder-Surfing* sogar das Passwort bei der Eingabe erkennt.

- Relevante Gegenmaßnahmen
  - Nutzung eines zweiten Faktors unterschiedlichen Typs (Besitz oder Inhärenz)
  - Einschränkung des Zugriffs auf die Container-Datei (z. B. offline Passwortmanager, zusätzlicher Schutz)

7.3.2 A02: Angreifer hat zeitlich begrenzten Zugriff auf das entsperrte Endgerät

- Erläuterung

Angreifer A02 kann für einen begrenzten Zeitraum auf den entsperrten Computer / das Mobilgerät der Nutzerinnen und Nutzer zugreifen, wodurch er insbesondere ungeschützte Passwortmanager auslesen kann. Technisch komplexe Angriffe, wie das Installieren von Malware oder das Erstellen eines Speicherabbilds, kann der Angreifer nicht durchführen. Das Kopieren der Passwortmanager-Datei ist in diesem Modell nicht erfasst, da es durch A04 abgedeckt ist.

- Beispielszenario

Ein Nutzer lässt sein Endgerät für kurze Zeit ungesperrt im Café liegen, während er zur Toilette geht. Die Tischnachbarin nutzt die Gelegenheit um "mal kurz reinzuschauen".

- Relevante Gegenmaßnahmen
  - Zeitbasierte Sperrung des Passwortmanagers (verhindert den Angriff nicht in jedem Fall, erhöht aber stark die Wahrscheinlichkeit, dass der PWM gesperrt ist)
  - Biometrie basierte Sperrung des Passwortmanagers

7.3.3 A03a: Angreifer kompromittiert Herstellerserver

- Erläuterung

Angreifer A03a kann den / die Server des Passwortmanager-Herstellers kompromittieren und dort vorhandene Daten kopieren sowie den Server manipulieren. Es wird angenommen, dass die Entwicklungsumgebung, die zugehörigen Repositorien sowie die Signaturzertifikate stärker geschützt sind und daher die ausgelieferte Software nicht manipuliert und mit Hintertüren versehen werden kann.

- Beispielszenario

Eine Serveradministratorin beim Hersteller eines Passwortmanagers ist bestechlich und übergibt ihre Zugangsdaten an eine kriminelle Organisation, welche daraufhin alle auf der Cloud des Herstellers gespeicherten Daten kopiert und den Server so manipuliert, dass alle Zugangsdaten der Nutzenden kopiert werden.

- Relevante Gegenmaßnahmen
  - Rein offline betriebene Passwortmanager
  - Trennung zwischen Authentisierungsinformationen an der Cloud und Masterpasswort
  - Near-Zero-Knowledge-Architektur, d.h. Daten sind nur einsehbar für Nutzende. Für den Hersteller sind Nutzerdaten eine Blackbox. Es kann z. B. nicht erraten werden, für welchen Service ein neues Credential angelegt wurde.

7.3.4 A03b: Supply-Chain-Attack

- Erläuterung

Angreifer A03b kann eine im Passwortmanager verwendete Softwarebibliothek manipulieren und somit manipulierten Code in den Passwortmanager einschleusen.

- Beispielszenario

Ein Passwortmanager bindet eine Open-Source Bibliothek zur Datenkompression ein. Die Bibliothek wird von nur einem einzigen freiwilligen Entwickler gepflegt, der diese irgendwann irrtümlich an einen Angreifer übergibt. Der Angreifer kann so manipulierten Code einspielen, der nach dem nächsten Update auch im Passwortmanager verwendet wird, siehe auch: https://en.wikipedia.org/wiki/XZ_Utils_backdoor (https://en.wikipedia.org/wiki/XZ_Utils_backdoor) (https://en.wikipedia.org/wiki/XZ_Utils_backdoor (https://en.wikipedia.org/wiki/XZ_Utils_backdoor)).

- Relevante Gegenmaßnahmen
  - Öffentlich verfügbare SBOMs
  - Secure-Software-Development (Library-Review and Version-Pinning, eigenes Paket-Repository)
  - Reduzierte Anzahl von Drittpaketen und Nutzung von etablierten und gut gepflegten Bibliotheken

7.3.5 A03c: Angriff auf Softwareentwicklungsprozess

- Erläuterung

Angreifer A03c kann einfache Angriffe auf die Entwicklungsumgebung für die Clientsoftware durchführen. Er kann Quellcode manipulieren und nicht abgesicherte Auslieferungsprozesse angreifen.

- Beispielszenario

Eine Softwareentwicklerin beim Hersteller eines Passwortmanagers ist bestechlich und schleust Schadcode in ein Modul der Passwortmanager Anwendung ein. Dies fällt im Entwicklungsprozess und in der Qualitätssicherung nicht auf und wird an die Kundinnen und Kunden ausgeliefert. Die manipulierten Passwortmanager bei allen Endkunden senden die gespeicherten Passwörter für bank.de (http://bank.de) an die Softwareentwicklerin.

- Relevante Gegenmaßnahmen
  - Schutzmechanismen im Softwareentwicklungsprozess
  - Signierte Software und Schutz der Signaturzertifikate
  - Open-Source & Reproducible Builds

7.3.6 A04: Angreifer hat Zugriff auf den Passwort-Container

- Erläuterung

Angreifer A04 ist in der Lage, die Passwort-Container Datei zu kopieren und nach seinem Belieben zu untersuchen.

- Beispielszenario

Ein Nutzer des Passwortmanagers gibt sein Endgerät zur Reparatur. Der Servicetechniker kann nach der Reparatur auf die gespeicherten Daten zugreifen, die Passwort-Container-Datei kopieren und im Nachgang über das eigene Gerät angreifen.

- Relevante Gegenmaßnahmen
  - Einsatz sicherer Kryptografie

7.3.7 A05: Auf dem Gerät des Nutzers ist eine Malware installiert

- Erläuterung

Angreifer A05 kann eine von ihm kontrollierte Schadsoftware mit Administratorrechten auf dem Endgerät des Nutzenden installieren und damit auf alle Dateien und geöffneten Prozesse zugreifen.

Ein kompletter Schutz gegen diesen Angriff ist nicht bekannt, spätestens bei der Nutzung kann der Angreifer die entschlüsselten Passwörter mitlesen. Denkbar wäre ein Mechanismus, der verhindert, dass ein Angreifer den kompletten Inhalt des Passwortmanagers auslesen kann und nur die tatsächlich genutzten Passwörter erhält.

- Beispielszenario

Im Urlaub wird einer Nutzerin ihr Telefon gestohlen. Um ihr digitales Rückflugticket ausdrucken zu können, muss sie ihren Passwortmanager in einem Internetcafé entsperren und das Passwort für den Account bei der Fluggesellschaft nutzen. Der Computer im Internetcafé ist mit einer Malware infiziert und alle für den Angreifer erreichbaren Daten werden abgezogen.

- Relevante Gegenmaßnahmen

Der Schutz ist ausgesprochen schwierig, nichtsdestotrotz könnte es Szenarien geben, in denen der Passwortmanager einen Großteil der Geheimnisse schützt - die Menge an exponierten Geheimnissen also einschränkt.

Eine Option zum Schutz ist die Nutzung eines Hardware-Security-Tokens als zweiten Faktor mit User-Presence-Check, sowie die getrennte Verschlüsselung aller Inhalte, sodass bei jedem User-Presence-Check nur ein Passwort ausgelesen werden kann.

7.3.8 A06: Angreifer kontrolliert eine Subdomain der Domain, die er angreifen will

- Erläuterung

Angreifer A06 hat die volle Kontrolle über eine Subdomain zu einer Domain, für die ein Passwort im Passwortmanager hinterlegt ist.

- Beispielszenario

Die Nutzerin studiert an einer Universität und hat daher im Passwortmanager einen Eintrag für beispiel-uni.edu (http://beispiel-uni.edu) abgelegt. Eine versierte Kommilitonin hat für ein Projekt die Domain area52.beispiel-uni.edu (http://area52.beispiel-uni.edu) angelegt und kontrolliert diese, sowie den darauf bereitgestellten Inhalt. Die angreifende Studentin schafft es, die Nutzerin des Passwortmanagers auf die Webseite unter area52.beispiel-uni.edu (http://area52.beispiel-uni.edu) zu locken.

- Relevante Gegenmaßnahmen
  - Auto-Fill-Mechanismus des Passwortmanagers mit exaktem Domain Matching