— Sicherheitsbewertung des Passwortmanagers heylogin

Abschlussbericht

Version: 1.2
Veröffentlichung: 04.05.2026

Erstellt von:
FZI Forschungszentrum Informatik
Stiftung des bürgerlichen Rechts
Haid-und-Neu-Str. 10-14
76131 Karlsruhe

Ansprechpartner: Niklas Goerke
E-Mail: goerke@fzi.de

– Inhaltsverzeichnis

1 Kontext und Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik hat zum 01.12.2025 die Ergebnisse einer Studie zur „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Passwortmanager“ [1] veröffentlicht. Das FZI Forschungszentrum Informatik als beauftragter Fachpartner hat diese Studie zusammen mit dem BSI durchgeführt. Die Veröffentlichung enthält neben den Prüfergebnissen von 10 Passwortmanagern auch das Prüfschema, das angesetzte Angreifermodell sowie weitere Informationen, die eine Nachprüfung weiterer Passwortmanager ermöglichen. Die Produkte der heylogin GmbH wurden in dieser Studie nicht betrachtet.

Im Nachgang beauftragte die heylogin GmbH das FZI mit der Durchführung einer Untersuchung nach den gleichen Maßstäben, wie sie in der Studie des BSI angelegt wurden. Das Prüfschema des BSI wurde für die Untersuchung von Passwortmanagern für Privatpersonen konzipiert. Die hier dargestellten Ergebnisse beziehen sich ausschließlich auf die heylogin Variante „Privat“.

Das hier vorliegende Dokument fasst die Ergebnisse dieser Untersuchung zusammen und stellt sie den Ergebnissen der initial untersuchten zehn Passwortmanager gegenüber.

Die in diesem Dokument beschriebenen Erkenntnisse beziehen sich auf das vom Auftraggeber veröffentlichte Security Whitepaper in Version 3.6, auf Antworten zu Rückfragen, die während des Untersuchungszeitraums gestellt wurden und Beobachtungen, die während der Interaktion mit der Software getätigt wurden. Nicht Bestandteil der Untersuchung war eine technische Überprüfung der Implementierung.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager_sicherheit_datenschutz.pdf

2 Management Summary

Die konzeptionelle Untersuchung des Passwortmanagers *heylogin* ergab keine grundsätzlichen Bedenken, die gegen die Nutzung sprechen, die Kritik konzentriert sich auf wenige Punkte. Bei der Betrachtung der Android App in Version 2026-01-08-27332de49 wurde festgestellt, dass Screenshots angefertigt werden können, auch während Passwörter im Klartext angezeigt werden. Weiterhin gibt es in der Android App kein automatisches Leeren der Zwischenablage, wenn Passwörter in diese kopiert werden. Das Kopieren in die Zwischenablage entspricht nicht dem eigentlich vorgesehenen Mechanismus von *heylogin*, kann aber dennoch in bestimmten Szenarien dazu führen, dass Nutzende ungewollt Geheimnisse weitergeben. Weiterhin existiert zwar eine Sperre für die Webapp, deren Timer auf vordefinierte Werte gesetzt werden kann, allerdings halten wir den standardmäßig gesetzten Wert von 2 Uhr morgens am Folgetag für zu hoch. Für spezifische Fälle ist das Domain Matching nicht restriktiv genug. Ein Angreifer, der eine Subdomain einer Domain kontrolliert, für welche Nutzende Logins gespeichert haben, könnte somit an die Logins gelangen. Weiterhin sollte geprüft werden, gespeicherte Passwörter hinsichtlich ihrer Qualität zu bewerten und einen entsprechenden Indikator anzubieten.

3 Gefährdungsanalyse

3.1 Prüfschema

Das zentrale Instrument der Untersuchung ist ein umfassendes Prüfschema. Es dient dazu, die Variante des Passwortmanagers *heylogin* für Privatanwendende anhand einer vordefinierten und einheitlichen Liste von Kriterien strukturiert zu beurteilen. Dieses Vorgehen stellt sicher, dass das untersuchte Produkt unter den gleichen Gesichtspunkten wie andere Produkte der Marktanalyse analysiert wird und die Ergebnisse mit diesen vergleichbar sind. Für die hier durchgeführte Untersuchung wurde das in der BSI-Studie veröffentlichte Prüfschema angewandt.

3.2 Ergebniskurzübersicht

In Tabelle 1 Ergebniskurzübersicht werden die wesentlichen Auffälligkeiten, die für die Beurteilung eines Passwortmanagers relevant sind, aufgeführt. Im Abschnitt Vollständiges Ergebnis befindet sich der Detailbericht der Untersuchung.

Name	heylogin
Untersuchte Version, Plattform und Veröffentlichungsdatum	Version 2026-01-08-27332de49, veröffentlicht am 08.01.2026, letzte Bearbeitung des Play-Store-Eintrags am 15.01.2026
Hersteller und Sitz des Herstellers	heylogin GmbH, Braunschweig, Deutschland
Lizenz	Kommerziell
Zugriffsmöglichkeit durch den Hersteller	Kein Zugriff
Zentrale Prüffeststellungen	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	Der Hersteller lieferte umgehend umfassende Antworten auf gestellte Fragen.
Einschätzung und Empfehlungen für Verbraucherinnen und Verbraucher	Insgesamt ergaben sich während der Untersuchung keine grundsätzlichen Bedenken, die gegen die Nutzung von heylogin sprechen. Verbraucherinnen und Verbraucher sollten für sich festlegen, welcher Zeitraum für eine zeitbasierte Sperrung des Passwortmanagers für ihre Bedürfnisse vertretbar ist.

Tabelle 1 Ergebniskurzübersicht

3.3 Vollständiges Ergebnis

Tabelle 2 Vollständige Ergebnisübersicht fasst die Ergebnisse der Sicherheitsuntersuchung zusammen.

	Eintrag	Ergebnis
	Basisinformationen	
1	Name	heylogin
2	Untersuchte Version, Plattform und Veröffentlichungsdatum	Android: Version 2026-01-08-27332de49, veröffentlicht am 08.01.2026, letzte Bearbeitung des Play-Store-Eintrags aber am 15.01.2026
3	Hersteller	heylogin GmbH
4	Eigenbeschreibung des Programms	"heylogin ist der erste Passwort-Manager mit hardwarebasierter Ende-zu-Ende-Verschlüsselung. Standardmäßig 2-Faktor-sicher, entwickelt und gehostet in Deutschland" Quelle: https://www.heylogin.com/de
5	Sitz des Herstellers	heylogin GmbH Sophienstr. 40 38118 Braunschweig
6	Lizenz	Kommerziell
7	Erstveröffentlichung	Dezember 2020
8	Datum des letzten Updates	Android App: 08.01.2026, Eintrag im Play Store: 15.01.2026

<table>
<tr>
<td>9</td>
<td>Entsprechen die dem Produkt beigefügten Informationen den Anforderungen des CRA Anhang II sowie BSI TR 03183-01 REQ_UD 1 - REQ_UD 6?</td>
<td>BSI TR 03183-01 ist ein "Living Document". Wir haben – wie beim ursprünglichen Passwortmanager-Projekt – Version 0.9 verwendet.
<table>
<tr><th>Eintrag</th><th>Antwort</th></tr>
<tr><td>CRA Anhang II Nr. 1</td><td>✅ Über den Browser > Einstellungen > Help Center > To heylogin.com > Impressum. Könnte in einem "About" leichter zu finden sein.</td></tr>
<tr><td>CRA Anhang II Nr. 2</td><td>✅ Über den Browser > Einstellungen > Help Center > Zu unserem Trust Center > Sicherheitsupdates > Letzte Sicherheitsupdates</td></tr>
<tr><td>CRA Anhang II Nr. 3</td><td>✅ Eindeutig identifizierbar als heylogin</td></tr>
<tr><td>CRA Anhang II Nr. 4</td><td>✅ Über den Browser > Einstellungen > Help Center > Zu unserem Trust Center</td></tr>
<tr><td>CRA Anhang II Nr. 5</td><td>❌</td></tr>
<tr><td>CRA Anhang II Nr. 6</td><td>❓ Applicable?</td></tr>
<tr><td>CRA Anhang II Nr. 7</td><td>Type of technical security support: ✅ Es gibt die Möglichkeit, im Trust Center Sicherheitsupdates zu abonnieren oder anzeigen zu lassen
End-date of the support period: ❌</td></tr>
<tr><td>CRA Anhang II Nr. 8 a)</td><td>❌</td></tr>
<tr><td>CRA Anhang II Nr. 8 b)</td><td>❌</td></tr>
<tr><td>CRA Anhang II Nr. 8 c)</td><td>❓ (Passiert über den Store für das mobile Endgerät automatisch)</td></tr>
<tr><td>CRA Anhang II Nr. 8 d)</td><td>✅ Über den Browser > Einstellungen > Help Center > Account & Produkt > heylogin verlassen</td></tr>
<tr><td>CRA Anhang II Nr. 8 e)</td><td>❌</td></tr>
</table>
</td>
</tr>
</table>

	Eintrag	Ergebnis	
		CRA Anhang II Nr. 8 f)	❌
		CRA Anhang II Nr. 9	❌
		BSI TR 03183-01 REQ_UD 1	✅ Über den Browser > Einstellungen > Help Center > To heylogin.com > Impressum. Könnte in einem "About" leichter zu finden sein.
		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	Type of technical security support: ✅ Es gibt die Möglichkeit, im Trust Center Informationen zu Sicherheitsupdates zu abonnieren oder anzeigen zu lassen End-date of the support period: ❌
		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?	N/A *Hinweis*: Es existiert kein Master-Passwort	
11	Welcher Algorithmus wird für die Bewertung der Qualität des Master-Passworts verwendet?	N/A *Hinweis*: Es existiert kein Master-Passwort	
12	Entsprechen die Indikatoren für die Bewertung der Qualität des Master-Passworts den Empfehlungen der NIST?	N/A *Hinweis*: Es existiert kein Master-Passwort	

	Eintrag	Ergebnis
13	Gibt es Vorgaben für die Qualität des Master-Passworts?	N/A *Hinweis*: Es existiert kein Master-Passwort
14	Kann das Master-Passwort geändert werden?	N/A *Hinweis*: Es existiert kein Master-Passwort
15	Können nach Änderung des Master-Passworts weiterhin mit dem alten Passwort Informationen aus dem neuen Container abgeleitet werden?	N/A *Hinweis*: Es existiert kein Master-Passwort
16	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Prozesses zur Änderung des Master-Passworts?	N/A *Hinweis*: Es existiert kein Master-Passwort
17	Kann eine zwei-Faktor-Authentisierung zum Entsperren des Passwort-Managers genutzt werden?	Der Hersteller argumentiert, dass der Passwortmanager standardmäßig 2FA bietet, da man das mobile Endgerät/den FIDO2-Schlüssel/das TPM besitzen (Possession Factor) und dieses/diesen mittels Biometrie (Biometric Factor) oder PIN (Knowledge Factor) entsperren muss.
18	Kann der Passwort-Manager durch andere Mechanismen als das Master-Passwort entsperrt werden?	Ja, der Passwort-Manger kann nur durch ein eigenes Verfahren durch ein verbundenes Smartphone entsperrt werden. *Hinweis*: Es gibt kein Master-Passwort.
19	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse der Zwei-Faktor-Authentisierung zum Entsperren des Passwort-Managers?	Nein
20	Gibt es eine Recovery-Option bei Verlust des Master-Passworts?	Ja *Hinweis*: Es existiert kein Master-Passwort. Es gibt die Möglichkeit, einen *Platform Backup Authenticator* und einen *Backup Code Authenticator* aufzusetzen. Der *Platform Backup Authenticator* verwendet die Backup API des mobilen Endgeräts (Android oder iOS). Der *Backup Code Authenticator* stellt einen 24-stelligen numerischen Code bereit, der zusammen mit einem Salt vom Server verwendet wird, um ein Backup Seed zu erstellen.

<table>
<tr><th></th><th>Eintrag</th><th>Ergebnis</th></tr>
<tr><td>21</td><td>Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Prozesses zum Recovery des Master-Passworts?</td><td>Nein

Hinweis: Der Recovery Code wird verschlüsselt auf dem Server gespeichert.</td></tr>
<tr><td>22</td><td>Welche kryptografischen Algorithmen werden verwendet und sind diese in ihrer Verwendung konform mit BSI TR-02102-1?</td><td>
<table>
<tr><th>Funktion</th><th>Algorithmus</th><th>TR-02102-1 compliant</th></tr>
<tr><td>Dient als KDF des Backup Code Authenticator</td><td>Argon2</td><td>❓ (Unklar, Argon2id zumindest compliant)</td></tr>
<tr><td>An allen Stellen, an denen symmetrische Krypto verwendet wird, zur Authentifizierung (Verschlüsselung der Vaults)</td><td>Poly1305</td><td>❓ (nicht explizit erwähnt)</td></tr>
<tr><td>An allen Stellen, an denen symmetrische Krypto verwendet wird, zur Verschlüsselung (Verschlüsselung der Vaults)</td><td>XSalsa20</td><td>❓ (nicht explizit erwähnt)</td></tr>
<tr><td>An allen Stellen, an denen asymmetrische Krypto verwendet wird (Verschlüsselung profileSeeds)</td><td>Curve25519</td><td>❓ (nicht explizit erwähnt)</td></tr>
<tr><td>Ableitung des Salts über die TweetNaCl.js-hash-Funktion. Erzeugt einen 32 Byte Hash.</td><td>SHA-256</td><td>✅</td></tr>
</table>
</td></tr>
<tr><td>23</td><td>Sind alle eingesetzten kryptographischen Algorithmen resistent gegen Brute-Force-Angriffe?</td><td>Ja</td></tr>
<tr><td>24</td><td>Erfolgt die Verschlüsselung mit einem Post-Quanten-Kryptographie Algorithmus?</td><td>Nein. Das Whitepaper schreibt hierzu selbst: "heylogin follows a post-quantum strategy, but is currently not fully post-quantum secure. This is because the asymmetric cryptographic mechanisms in use are based on Curve25519".</td></tr>
</table>

<table>
<tr><th></th><th>Eintrag</th><th>Ergebnis</th></tr>
<tr><td>25</td><td>Wird selbst implementierte Kryptographie genutzt?</td><td>Nein. Das Paper erwähnt, dass für Krypto die TweetNaCl.js-Bibliothek verwendet wird. Da diese aber kein Argon2 unterstützt (obwohl TweetNaCl das tut), wird für Argon2 eine "separate implementation" verwendet. Dafür wird das Argon2Kt Binding für die Referenzimplementierung von Argon2 in C verwendet, die die Password Hashing Competition gewonnen hat.</td></tr>
<tr><td>26</td><td>Wird der komplette Inhalt vollständig verschlüsselt?
Passwörter
Benutzernamen
URLs
Favicons
Dateien</td><td>Ja
Aus dem Whitepaper v3.5, Section 3.2 "What we encrypt and how":<table><tr><th>Encryption layer</th><th>Data types</th><th>Access</th></tr><tr><td>Transport secure (TLS)</td><td>Organization name, account emails, IP addresses, unlock times, activity times, device data</td><td>Visible to provider as required for account management, troubleshooting, and support</td></tr><tr><td>1st layer end-to-end encryption</td><td>Usernames (stored with logins), websites/domains, team names, unprotected custom fields</td><td>Available on all paired devices, even when locked (used for overlays)</td></tr><tr><td>2nd layer end-to-end encryption</td><td>Passwords, TOTP secrets, protected custom fields</td><td>Available only on paired and unlocked devices</td></tr><tr><td>Additional encryption at rest</td><td>Server backups</td><td>Provides additional protection by keeping server backups inaccessible even if backup storage is breached</td></tr></table></td></tr>
<tr><td></td><td>Features</td><td></td></tr>
<tr><td>27</td><td>Gibt es einen Passwortgenerator?</td><td>Ja</td></tr>
<tr><td>28</td><td>Welcher Algorithmus wird für die Bewertung der Qualität von gespeicherten Passwörtern verwendet?</td><td>Die Qualität der gespeicherten Passwörter wird nicht bewertet.</td></tr>
</table>

	Eintrag	Ergebnis
29	Entsprechen die Indikatoren für die Bewertung der Qualität von Passwörtern den Empfehlungen der NIST?	N/A *Hinweis*: Die Qualität der gespeicherten Passwörter wird nicht bewertet.
30	Gibt es die Möglichkeit, Daten zum Ausfüllen von Authentisierungsinformationen an andere Programme zu übertragen (Browser, Apps)?	Ja, via Browser Extensions.
31	Mit welchen gängigen Browsern ist der Passwort-Manager kompatibel?	Es gibt Browser Extensions für • Google Chrome • Mozilla Firefox • Safari • Microsoft Edge
32	Wird Host, Domain oder Subdomain gematcht?	Beispiel mit dem Passwort-Eintrag für *dash.example.com* • *dash.example.com*: wird vorgeschlagen • auth.dash.example.com: wird vorgeschlagen • *mail.example.com*: wird nicht vorgeschlagen • *example.com*: wird nicht vorgeschlagen • *example.com.evil.de*: wird nicht vorgeschlagen
33	Werden Nutzername und Passwort beim Laden der Website automatisch ausgefüllt oder braucht es Nutzerinteraktionen?	Der Login wird automatisch in einem Overlay vorgeschlagen, standardmäßig braucht es noch einen Klick für das Starten des Login-Vorgangs.
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?	Nein. Falsche Passwörter können nicht ausgewählt werden, nur in die Zwischenablage kopiert und manuell eingefügt.
35	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse der Verbindung des Passwort-	Ja Die zweischichtige Ende-zu-Ende-Verschlüsselung ermöglicht es, auf einem gepairten Gerät Logins vorzuschlagen, auch wenn dieses gesperrt ist (Verwendung der Informationen für das Overlay). Ein Angreifer mit Zugriff auf

	Eintrag	Ergebnis
	Managers mit dem Browser sowie dem Matching der Webseite im Browser?	den gesperrten Passwortmanager kann somit lernen, ob für eine Seite ein Login existiert. Das Subdomain-Matching sollte restriktiver sein, siehe Antwort zu Frage 32 und Angreifermodell A06 (Anhang: Angreifermodelle).
36	Welche Sicherheitsmechanismen des Betriebssystems werden verwendet (z.B. TPM, Lockscreen Trigger), wie werden diese jeweils verwendet?	Auf dem Mobile Authenticator wird das TPM genutzt, um die verschiedenen Seeds zu speichern.
37	Wird die Zwischenablage automatisch geleert, wenn die vom PWM vorgesehene Funktion zum Kopieren verwendet wird? Wenn ja, nach welcher Zeit?	In der Webapp: Ja In der Android App: Beim manuellen Kopieren in die Zwischenablage wird diese nicht geleert.
38	Sperrt sich der PWM automatisch nach einer gewissen Zeit? Wenn ja, nach welcher Zeit?	Teilweise. Layer 1 wird auf einem gepairten Gerät nicht gesperrt, Layer 2 sperrt sich standardmäßig um 2 Uhr morgens am Folgetag. Es gibt die Einstellungsmöglichkeiten: • 5 Minuten • 15 Minuten • eine Stunde • zwei Stunden • acht Stunden • ein Tag
39	Gibt es eine Funktion zum Export von Passwörtern?	Ja
40	In welche verschlüsselten und unverschlüsselten Formate kann exportiert werden?	Unverschlüsselt: • CSV
41	Gibt es eine Funktion zum sicheren Teilen von Passwörtern mit anderen Personen oder Instanzen?	Nein, nicht in der Version für private Nutzende.

	Eintrag	Ergebnis
42	Wie ist die Funktion zum Teilen von Passwörtern mit anderen Personen oder Instanzen umgesetzt?	N/A
43	Gibt es eine Funktion, um Passwörter gegen bekannte Leaks zu prüfen? (z. B. "*Have I Been Pwned*"?)	Ja
44	Läuft diese Prüfung automatisch?	Ja
45	Unterstützt der Passwort-Manager die Verwaltung von zusätzlichen Authentisierungsfaktoren für Zwei-Faktor-Authentisierung bei anderen Diensten (z.B. TOTP)?	Ja *Hinweis*: Der Passwortmanager unterstützt die Verwaltung von TOTP
	Synchronisation	
46	Können gespeicherte Daten über eine Cloud synchronisiert werden?	Ja, die herstellereigene Cloud.
47	Können Nutzende den Speicherort für die Online-Synchronisation frei wählen, welche stehen zur Auswahl?	Nein
48	Betreibt der Hersteller einen angebotenen Speicherort selbst? Falls nein: Welche Anbieter nutzt er?	Der Hersteller nutzt den Dienstleister Hetzner, um das Produktionssystem in Nürnberg zu hosten. Ein weiterer Standby-Server (Für Failover in Notfällen) sitzt in Falkenstein. Unabhängige Backups werden bei IONOS (Frankfurt) gespeichert. Quelle: https://www.heylogin.com/de/trust-center Es gibt eine Liste an Unterauftragsverarbeitern: https://www.heylogin.com/de/unterauftragsverarbeiter Hier wird zusätzlich die Heinlein Hosting GmbH (mailbox.org) für den Versand von E-Mails genannt.

	Eintrag	Ergebnis
49	In welchem Land werden Daten gespeichert?	Deutschland
50	Wie authentisieren sich Nutzende gegenüber dem vom Hersteller angebotenen Speicherort?	Mittels des *login*-Schlüsselpaares, das aus dem Authenticator Seed abgeleitet wird.
51	Werden Maßnahmen eingesetzt, um Brute-Force-Angriffe zu unterbinden und wie sind diese umgesetzt?	Aus dem Whitepaper, v3.6: Das TPM auf dem Endgerät limitiert die Angriffsrate, eine vollständige Suche über den Seed wird dort als unmöglich bezeichnet. Da die Authentifizierung gegenüber dem Server sowie die Verschlüsselung des Vaults passwortlos geschieht, müsste eine vollständige Suche über den gesamten Key Space erfolgen.
52	Wird Transportverschlüsselung und Zertifikat-Pinning korrekt umgesetzt?	Transportverschlüsselung: Ja Zertifikat-Pinning: Ja
53	Was wird synchronisiert: Container oder Einzelobjekte?	Die Logins werden im Vault als Commits gespeichert. Commits besitzen Metadaten, die es ermöglicht sie (nach Timestamp) zu sortieren. Commits spiegeln den Inhalt des gesamten Vaults wider und verhalten sich analog zu Commits in Versionskontrollsystemen wie git.
54	Wie werden Konflikte bei der Synchronisation gelöst?	Zeitlich letzter Edit überschreibt.
55	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Synchronisationsmechanismus? Welche Informationen kann der Hersteller, beziehungsweise der Serverbetreiber lernen?	Nein.
	Modellierung und Sicherheitstests	
56	Gibt es Auffälligkeiten in Modellierung und Bedrohungsanalyse des Passwort-Managers?	Modelliert wurde die Resistenz gegen verschiedene Angreifermodelle. Diese sind im Anhang erläutert.

	Eintrag	Ergebnis			
		Angreifer	**Kurzbeschreibung**	**Resistent in Standardeinstellung**	**Erläuterung**
		A01	Nur Master-Passwort bekannt	✅	Es existiert kein Master-Passwort, daher ist der PWM resistent gegen Angriffe wie Shoulder Surfing.
		A02	Zugriff auf entsperrtes Gerät	❗	Es gibt zwar eine Sperre für den Browser, aber standardmäßig ist die Sperrung des Browsers auf 2 Uhr am Folgetag gesetzt, was nach unserer Einschätzung zu hoch angesetzt ist.
		A03a	Herstellerserver kompromittiert	✅	Die relevanten Public Keys von privaten Vaults können nicht einfach ausgetauscht werden, da sie vom Besitzer digital signiert sind.
		A03b	Supply-Chain-Attack	❗	Es gibt keine öffentlich verfügbaren SBOMs. Letztes npm Package Update von TweetNaCl.js 2020, Lock File hat Zirkumflexes.
		A03c	Entwickler kompromittiert	✅	Der Softwareherstellungsprozess wird regelmäßig auditiert.
		A04	Zugriff auf gesperrten Container	✅	Es werden keine schwachen kryptografischen Algorithmen für die Verschlüsselung eingesetzt.

<table>
<tr><th></th><th>Eintrag</th><th colspan="4">Ergebnis</th></tr>
<tr><td></td><td></td><td>A05</td><td>Malware auf Endgerät</td><td>❗</td><td>Es wird der Android-KeyStore verwendet. Die Zwischenablage wird aber nicht automatisch geleert und Screenshots nicht verhindert.</td></tr>
<tr><td></td><td></td><td>A06</td><td>Kontrolle über Subdomain</td><td>❌</td><td>Siehe Eintrag 32</td></tr>
<tr><td>57</td><td>Für Android-Apps: Werden alle Tests der OWASP MASVS-RESILIENCE-Klasse erfüllt?</td><td colspan="4"><table><tr><th>Prüfnummer</th><th>Konformität</th></tr><tr><td>0224</td><td>✅</td></tr><tr><td>0225</td><td>✅</td></tr><tr><td>0226</td><td>✅</td></tr><tr><td>0227</td><td>✅</td></tr><tr><td>0247</td><td>✅</td></tr></table>
Ja</td></tr>
<tr><td>58</td><td>Für Android-Apps: Können sensitive Daten durch andere Apps gelesen werden?</td><td colspan="4">Screenshots sind möglich, auch bei angezeigtem Passwort. Die Zwischenablage wird nicht standardmäßig geleert.</td></tr>
<tr><td></td><td colspan="5">Prozesse und Vorgehen des Herstellers</td></tr>
<tr><td>59</td><td>Wurden bereits Sicherheits-Audits für dieses Produkt durchgeführt?</td><td colspan="4">Ja</td></tr>
<tr><td>60</td><td>Wer hat die Sicherheits-Audits beauftragt?</td><td colspan="4">heylogin</td></tr>
<tr><td>61</td><td>Wurden bereits Penetrationstests für dieses Produkt durchgeführt?</td><td colspan="4">Ja</td></tr>
</table>

	Eintrag	Ergebnis
62	Wer hat diese Penetrationstests beauftragt?	heylogin
63	Gab es bereits erfolgreiche Angriffe auf den Passwort-Manager?	Nein
64	Falls ja: Wie reagierte der Hersteller auf den Angriff?	N/A
65	Wie reagiert der Hersteller auf Schwachstellen?	Es gibt sowohl eine security.txt als auch eine Infoseite: https://www.heylogin.com/de/security. Schwachstellenmeldungen sind willkommen.
66	Werden öffentlich Informationen zu Sicherheitsaktualisierungen bereitgestellt?	Ja. Auf der Seite https://www.heylogin.com/de/security können die letzten Sicherheitsupdates eingesehen werden. Außerdem existiert auf derselben Seite die Möglichkeit, sich für Sicherheitsupdates via E-Mail einzutragen.
67	Existiert ein sicherer Updatekanal?	Ja, die App wird über Google Play oder den Apple App Store ausgerollt.
68	Existiert ein öffentlich dokumentiertes Konzept für die koordinierte Offenlegung von Schwachstellen sowie ein Kontaktpunkt dazu?	• Auf der Website findet man einen Link zu Schwachstellenmeldungen: https://www.heylogin.com/de/schwachstellenmeldung ○ Dort ist sowohl eine E-Mail-Adresse, ein OpenPGP-Schlüssel und die Vulnerability Disclosure Policy angegeben • Es gibt eine security.txt

Tabelle 2 Vollständige Ergebnisübersicht

4 Erweiterte Ergebnisübersicht

Die folgende Tabelle ist eine Kopie der Ergebnisse der BSI Studie, erweitert um die Ergebnisse für *heylogin* in der letzten Spalte

Produkt	1Password	Avira Password Manager	Chrome Password Manager	Keepass 2Android	KeePass XC	Mozilla Firefox Password Manager	mSecure Password Manager	Pass Securium	SecureSafe Password-Manager	S-Trust Password Manager	heylogin
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.	Version 2026-01-08-27332de49
Sicherheitstechnische Eigenschaften											
Verwendung eines Masterpassworts in der Standard-konfiguration	Ja	Ja	Ja	Ja	Ja	Nein[2]	Ja	Ja	Ja	Ja	Nein[3]
Wiederherstellungsoption bei Verlust des Masterpassworts	Ja	Nein[4]	Nein[5]	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Ja
Kann mit zweitem Faktor geschützt werden	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

[2] Anstelle des Masterpassworts wird die Windows-Authentifizierung verwendet, dies ist in diesem Kontext vergleichbar.
[3] heylogin verwendet ein verbundenes Smartphone zum Entsperren anstelle eines Master-Passworts.
[4] Die vorhandene Wiederherstellungsoption über Biometrie sollte aus Sicherheitsgründen deaktiviert werden.
[5] Nutzende sollten eine eigene Passphrase setzen, eine Wiederherstellungsoption ist dann nicht mehr vorhanden.

Unterstützt Verwaltung zweiter Faktoren[6]	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Nein	Nein	Ja
Automatisches Leeren der Zwischenablage	Ja[7]	Ja	Nein	Ja	Ja	Nein	Ja[7]	Nein	Ja	Ja	Nein
Automatische Sperre nach Zeitüberschreitung in der Standardkonfiguration	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja
Cloud-Synchronisation[8]	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Prüfung gegen Leaks	Ja	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Nein	Nein	Ja
Export von Passwörtern	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja
Zentrale Prüffeststellung											
Der komplette Inhalt wird verschlüsselt.	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Ja
Nach Änderung des Masterpassworts wird der komplette Inhalt verschlüsselt	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Ja[9]
Hersteller kann auf die Daten zugreifen.[10]	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Ja	Nicht bewertbar	Nicht bewertbar	Nein

[6] Verwaltung von zusätzlichen Authentisierungsfaktoren für 2FA bei anderen Diensten.
[7] Wird bei aktuellen Android Versionen vom Betriebssystem übernommen.
[8] Können gespeicherte Daten über eine einfach aktivierbare Funktion mit einer vom Hersteller oder Drittanbieter betriebenen Cloud synchronisiert werden?
[9] Eine Neuverschlüsselung findet statt, sobald ein Push Authenticator entfernt wurde und eine Änderung an den Logins vorgenommen wird.
[10] Die Einträge beziehen sich auf die Standardkonfiguration bei aktivierter Synchronisation.

Es werden ausschließlich sichere, korrekt konfigurierte kryptografische Algorithmen eingesetzt.[11]	Ja, mit geringen Abweichungen	Unbekannt[12]	Unbekannt, nutzt Betriebssystemfunktionen	Ja, mit geringen Abweichungen	Ja, mit geringen Abweichungen	Ja, mit geringen Abweichungen	Unbekannt, mindestens geringe Abweichungen	Nein	Nein	Nein	Ja, mit geringen Abweichungen

Tabelle 3 Erweiterte Ergebnisübersicht. Weitere Erläuterungen und Hintergründe finden sich in der Marktanalyse[13].

[11] Im Sinne der BSI TR-02102-1.
[12] Einige Informationen konnten im Rahmen der Prüftiefe nicht erhoben werden.
[13] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager.pdf

5 Anhang: Angreifermodelle

5.1 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)

5.2 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

5.3 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.

5.4 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).

- 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

5.5 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

5.6 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

5.7 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.

5.8 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