MATERNA

Whitepaper

Passwort-Manager absichern

Architektur der Sicherheit:
Wie moderne Passwort-Manager Daten schützen

MATERNA

Passwort-Manager haben die Aufgabe, Passwörter sicher zu speichern, zu verwalten und automatisch einzusetzen. Daher müssen sie besonders abgesichert werden. Der benutzerdefinierte Baustein „APP.bd.8 Passwort-Manager“ zeigt, welche Anforderungen Passwort-Manager umsetzen sollten, um die Vertraulichkeit, Integrität und Verfügbarkeit der Kennwörter zu erhalten. Dieser Baustein wurde im Rahmen der Bachelor-Arbeit „Absicherung von Passwort-Managern auf Basis einer Risikoanalyse“ von Jannik Schonefeld, Consultant bei Materna, entwickelt.

1. Beschreibung

1.1. Einleitung

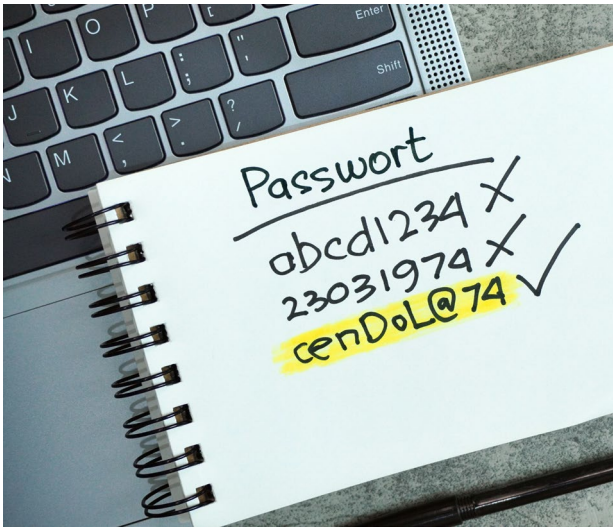
Passwörter sind eine der populären Methoden zur Authentifizierung in einer digitalen Welt. Aus einer sicheren Nutzung von Passwörtern resultiert die Herausforderung, sich für verschiedene Konten unterschiedliche Kennwörter zu merken, die ausreichend sicher gegenüber unbefugten Zugriffen sind. Da Menschen eine Vielzahl zufälliger Abfolgen von Symbolen nicht in Erinnerung behalten können, werden sich wiederholende, leicht merkbare und gleichzeitig unsichere Passwörter verwendet. Diese führen dazu, dass unbefugte Personen in Konten eindringen und sensible Daten auslesen oder schadhafte Handlungen ausführen können.

Um dem Problem entgegenzuwirken, existieren Passwort-Manager, welche die Generierung, Speicherung und das Abrufen der Zugangsdaten für den Nutzenden übernehmen. Die Kennwörter werden in einer Datenbank abgelegt, die mit einem Masterpasswort geöffnet wird. Der Anwendende muss sich daher nicht viele komplexe Passwörter merken, sondern kann mit einem einzigen Kennwort alle anderen abrufen.

Passwort-Manager bieten je nach System verschiedene Funktionen wie die Synchronisierung der Datenbank über verschiedene Geräte, das automatische Ausfüllen von Zugangsdaten auf Internetseiten sowie die Nutzung biometrischer Sensoren zur Authentifizierung. Außerdem können Zugangsdaten durch eine strukturierte Rollenverwaltung mit anderen Personen geteilt werden. Die Kennwortverwaltung ist daher keine alleinstehende Anwendung, sondern lässt sich auf vielfältige Weise in ein System integrieren.

Für Passwort-Manager stehen verschiedene Architekturmodelle zur Verfügung. Neben lokalen und On-Premises Datenbanken sind Browser-Erweiterungen und Cloud-Lösungen weit verbreitet. Jedes dieser Modelle hat unterschiedliche Anwendungsbereiche, die von der Anzahl der Nutzenden, der verwendeten Infrastruktur und den benötigten Sicherheitsanforderungen abhängen.

Zugleich können die zahlreichen Funktionen innerhalb der Programme Schwachstellen bieten, die von unbefugten Personen zur Extrahierung von Zugangsdaten ausgenutzt werden können. Passwort-Manager verwalten sensible Informationen an einer zentralen Stelle, sodass diese ein attraktives Angriffsziel darstellen.



1.2. Zielsetzung

Ziel dieses Bausteins ist es, Passwort-Manager auf eine Weise abzusichern, sodass weder die Vertraulichkeit noch die Integrität und Verfügbarkeit der Kennwörter gefährdet sind. Dazu enthält der Baustein Anforderungen, die bei einer Planung, Anwendung und Administrierung einer Kennwortverwaltung zu beachten und umzusetzen sind.

1.3. Abgrenzung und Modellierung

Der Baustein APP.bd.8 *Passwort-Manager* ist auf jeden im Informationsverbund eingesetzten Passwort-Manager anzuwenden.

Dieser Baustein bezieht sich auf die Nutzung und Verwaltung von Passwort-Managern sowie deren technische Integration in bestehende Systeme.
Dabei werden die verschiedenen Speicherungsformen (lokal und dezentral) für Zugangsdaten berücksichtigt. Nicht betrachtet wird die Absicherung der zugrunde liegenden Endgeräte, auf denen der Passwort-Manager betrieben wird, auf die dieser aber keinen Einfluss hat. Die Sicherheit dieser Systeme wird beispielsweise durch SYS.2.1 *Allgemeiner Client* modelliert. Der Baustein geht ebenso nicht auf die Anforderungen für Datenbanken zum Speichern von Zugangsdaten ein, wozu APP.4.3 *Relationale Datenbanken* modelliert wird. Ergänzend zu den Anforderungen dieses Bausteins müssen die Anforderungen des übergeordneten Bausteins APP.6 *Allgemeine Software* umgesetzt werden. Nicht Bestandteil des Bausteins ist die Sicherheit und Regelung des Passwortgebrauchs, welche in ORP.4 *Identitäts- und Berechtigungsmanagement* modelliert wird.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.bd.8 *Passwort-Manager* von besonderer Bedeutung.

2.1. Kein Zugriff auf die Passwortdatenbank

Ist für den Zugriff auf den Passworttresor eine Verbindung zum Datenbankserver erforderlich, kann durch einen Ausfall dieser Verbindung (z.B. durch den Ausfall der Netzwerkverbindung) der Nutzende nicht mehr auf die gespeicherten Passwörter zugreifen. Aufgrund der Komplexität der Kennwörter sind diese ebenfalls nicht in Erinnerung des Anwendenden, sodass keine Anmeldung möglich ist. Somit ist die Verfügbarkeit des Passwort-Managers eingeschränkt.

2.2. Unzureichende Verschlüsselung der Daten im Speicher

Infolge eines Softwarefehlers sind die Passwörter im Speicher des Endgerätes unverschlüsselt oder mit einer nicht sicheren Verschlüsselung abgelegt. Aufgrund der schwachen kryptografischen Absicherung kann eine unbefugte Person trotz fehlender Kenntnis über das Masterpasswort die Zugangsdaten auslesen, indem ein Speicherabbild erstellt und dieses ausgewertet wird. Als Konsequenz ist die Vertraulichkeit der Passwörter nicht mehr gewährleistet.

2.3. Diebstahl oder Verlust der Passwortdatenbank

Das Gerät mit der gespeicherten Passwortdatenbank wird durch einen Diebstahl entwendet beziehungsweise geht verloren. Die Gefährdung betrifft besonders lokale Passwort-Manager, da diese die Zugangsdaten nicht auf weiteren Geräten ablegen. Durch den Verlust hat der Anwendende keinen Zugriff mehr auf die gespeicherten Kennwörter. Gleichzeitig kann gegebenenfalls eine unbefugte Person bei unzureichender Absicherung der Datenbank durch den physischen Zugriff die Passwörter auslesen.

2.4. Unzureichende Authentifizierung beim Öffnen des Passworttresors

Sind die Authentifizierungsverfahren zum Öffnen des Passworttresors nicht ausreichend abgesichert, können Unbefugte auf die Datenbank mit den gespeicherten Informationen zugreifen. Als Folge können Kennwörter aus dem Passwort-Manager ausgelesen und geändert werden, sodass alle Sicherheitsziele nicht mehr gewährleistet sind.

2.5. Automatisches Ausfüllen auf gefälschten Internetseiten

Fügt der Passwort-Manager auf unsicheren und gefälschten Internetseiten die gespeicherten Passwörter automatisch ein, ist die Vertraulichkeit der Zugangsdaten nicht mehr gewährleistet. Im schlimmsten Fall werden alle Kennwörter aus der Datenbank durch das automatische Ausfüllen unbemerkt auf der gefälschten Seite eingegeben, da der Nutzende oftmals keine manuelle Bestätigung zum Einfügen der Passwörter geben muss.

2.6. Unbeabsichtigte Änderung oder Löschung von Passwörtern

Da Nutzende die Kennwörter innerhalb des Passwort-Managers bearbeiten und löschen können, besteht das Risiko der unbeabsichtigten Veränderungen von Passworteinträgen. Aufgrund der Komplexität der Zugangsdaten kennt der Anwendende das ursprüngliche, korrekte Passwort nicht. Wenn dieses nun verändert wird, werden sowohl die Verfügbarkeit als auch die Integrität der Daten verletzt und Anmeldevorgänge können nicht abgeschlossen werden.

2.7. Fehlfunktion durch Softwareupdate

Nach einem Softwareupdate des Passwort-Managers ist die einwandfreie Funktion der Anwendung nicht mehr gegeben. Zu möglichen Gründen zählt, dass die Änderungen nicht vollständig getestet wurden oder das Update nicht kompatibel mit allen Funktionen der Kennwortverwaltung ist. Dadurch ist der Betrieb des Passwort-Managers nicht einwandfrei oder weist Sicherheitslücken auf, durch die Unbefugte die Sicherheitsziele der Anwendung gefährden.

2.8. Fehlbedienung des Passwort-Managers

Sind die Anwendenden des Passwort-Managers nicht ausreichend in der Nutzung des Passwort-Managers geschult, kann dies zu einer Fehlbedienung führen. Kennwörter können ungewollt geteilt oder nicht ausreichend sicher gewählt werden. Zudem können Sicherheitseinstellungen durch mangelndes Wissen deaktiviert werden, sodass unbefugte Personen Zugriff auf die Passwörter erhalten. Als Konsequenz sind sowohl die Vertraulichkeit als auch die Verfügbarkeit und Integrität der Daten beeinträchtigt.

2.9. Missbrauch durch privilegierte Nutzende

Die Verwaltung des Passwort-Managers erfolgt durch Administrierende mit höheren Berechtigungen, um den Betrieb und die Bereitstellung der Dienste sicherzustellen. Diese privilegierten Nutzenden besitzen ohne entsprechende Gegenmaßnahmen Zugriff auf die Kennworttresore und können gespeicherte Daten einsehen, ändern oder löschen. Ein Missbrauch der Berechtigungen kann daher alle Sicherheitsziele beeinträchtigen.

2.10. Auslesen der Passwörter durch Schadsoftware

Schadsoftware auf dem Gerät kann die gespeicherten Kennwörter auslesen. Ursachen dafür können Keylogger sein, welche die Eingabe des Masterpasswortes mitschneiden. Auch die Zwischenablage für das Abrufen und Eingeben der Zugangsdaten kann von anderen Programmen ausgelesen werden. Zuletzt können die Passwörter auch manipuliert werden, sodass die Vertraulichkeit, Verfügbarkeit und Integrität der Passwörter bedroht sind.

2.11. Verlust des Masterpasswortes

Die Passwortdatenbank wird mit einem Masterpasswort als Authentifizierungsmethode abgesichert. Falls der Anwendende dieses vergisst oder verliert, ist ein Öffnen des Kennworttresors nicht möglich, da die Authentifizierung nicht erfolgreich abgeschlossen werden kann. Der Nutzende kann ohne Masterpasswort nicht auf die Passwörter in der Datenbank zugreifen, sodass die Verfügbarkeit nicht mehr gegeben ist.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.bd.8 *Passwort-Manager* aufgeführt. Der Informationssicherheitsbeauftragter (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	ISB, Anwendende des Passwort-Managers

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.bd.8 *Passwort-Manager* vorrangig erfüllt werden.

APP.bd.8.A1 Planung des Einsatzes des Passwort-Managers (B)
Die Institution MUSS den Einsatz des Passwort-Managers planen. Die Institution MUSS die Planung für die Kennwortverwaltung in einer Dokumentation festhalten. Die Institution MUSS den Passwort-Manager in das Sicherheitskonzept integrieren.

Die Institution MUSS die Risiken, die durch die Kennwortverwaltung entstehen, identifizieren und bewerten. Die für den Passwort-Manager relevanten internen und externen Anforderungen MÜSSEN identifiziert und bei der Planung berücksichtigt werden.

Die Institution MUSS sicherstellen, dass ausschließlich Software aus sicherer Herkunft verwendet wird. Es MUSS sichergestellt sein, dass aktuelle Updates und eine technische Betreuung des Programms durch den Hersteller zur Verfügung stehen.

Es MUSS definiert werden, welche Funktionen der Passwort-Manager bereitstellen soll und auf welche Weise die Daten gespeichert werden (etwa lokal, Cloud, On-Premises, Browser-Erweiterung). Es MUSS definiert sein, wie weit die Integration des Passwort-Managers in bestehende Systeme der Institution erfolgt.

Die Institution MUSS Verantwortlichkeiten zur Administration des Passwort-Managers festlegen.

APP.bd.8.A2 Umsetzung von Richtlinien (B)
Die relevanten Richtlinien der Institution MÜSSEN im Betrieb des Passwort-Managers berücksichtigt werden.

APP.bd.8.A3 Verschlüsselte Speicherung aller Daten auf Endgeräten (B)
Auf jedem Datenträger der Endgeräte MÜSSEN alle Daten (Passwörter, Benutzernamen, Internetseiten, Kontoinformationen, Statistiken über die Datenbank, etc.) verschlüsselt gespeichert werden.

Die Verschlüsselung MUSS sichere kryptografische Verfahren nutzen (vgl. BSI TR-02102-1).

Falls die Zugangsdaten für eine Handlung des Passwort-Managers im Arbeitsspeicher unverschlüsselt abgelegt werden, MÜSSEN die Daten bei Beendigung der Ausführung unverzüglich überschrieben werden. Es DÜRFEN KEINE Informationen der Kennwortverwaltung dauerhaft im Klartext im Arbeitsspeicher liegen.

APP.bd.8.A4 Absicherung der Kommunikation (B)
Die Kommunikation zwischen Passwort-Manager und seiner Datenbank sowie zwischen Passwort-Managern untereinander MUSS geschützt erfolgen, das heißt, es dürfen nur sichere Protokolle (Authentifizierungs-, Übertragungs- und Kommunikationsprotokolle) genutzt werden.

Bei nicht lokalen Passwort-Managern MUSS die Kommunikation Ende-zu-Ende verschlüsselt sein. Übertragungen, die nicht Ende-zu-Ende verschlüsselt sind, MÜSSEN aufgrund der Vertraulichkeit der Zugangsdaten abgelehnt werden.

Der Anwendende DARF NICHT die Einstellungen zur Kommunikationssicherheit des Passwort-Managers ändern können.

Die Ende-zu-Ende-Verschlüsselung MUSS beide Kommunikationsparteien gegenseitig authentifizieren.

APP.bd.8.A5 Umsetzung des Zero-Knowledge-Prinzips (B)
Serverbasierte Passwort-Manager MÜSSEN das Zero-Knowledge-Prinzip umsetzen, das heißt, alle Zugangsdaten, die an einen Server gesendet werden, MÜSSEN vorher auf dem Client verschlüsselt werden. Der Client DARF NICHT den kryptografischen Schlüssel weitergeben.

Es DÜRFEN KEINE Klartextdaten auf dem Server gespeichert werden. Es DARF KEINE Entschlüsselung der sensiblen Daten auf dem Server möglich sein.

APP.bd.8.A6 Sicheres Ausfüllen mit Interaktion des Benutzenden (B)
Passwort-Manager, die die Funktion des automatischen Ausfüllens bieten, DÜRFEN NICHT die Zugangsdaten ohne Überprüfung der Internetseite oder der Anwendung automatisch einfügen, das heißt, für ein sicheres Ausfüllen muss

- ein Abgleich der Domains erfolgen.
- das automatische Ausfüllen unterbunden werden, falls die Domains nicht übereinstimmen.
- das Einfügen von Zugangsdaten unterbunden werden, falls das Zertifikat der Internetseite ungültig ist.

Das automatische Ausfüllen der Passwörter MUSS eine aktive Interaktion mit dem Benutzenden erfordern, damit Kennwörter nur mit ausdrücklicher Zustimmung des Anwendenden eingefügt werden.

Passwörter MÜSSEN in sichtbare und aktive Eingabefelder eingesetzt werden, sodass versteckte Felder oder unsichtbare Elemente nicht befüllt werden.

Der Passwort-Manager MUSS das Kennwort direkt in das Eingabefeld einfügen, ohne es an anderer Stelle temporär zu speichern. Der Passwort-Manager MUSS das automatische Einfügen von Zugangsdaten in Inlineframe auf Internetseiten unterbinden.

Falls der Passwort-Manager die Zwischenablage des Gerätes nutzt, MUSS diese zeitnah gelöscht oder überschrieben werden.

Die Nutzenden SOLLTEN die Option haben, das automatische Ausfüllen generell oder für bestimmte Ziele zu deaktivieren.

APP.bd.8.A7 Sicheres Masterpasswort (B)
Es MUSS eine Richtlinie für das Masterpasswort geben, die alle Anforderungen an ein sicheres Masterpasswort zusammenfasst. Die Vorgaben MÜSSEN technisch im Passwort-Manager erzwungen werden.

Das Masterpasswort MUSS maßgeblich in die Berechnung des Schlüssels zur Chiffrierung der Passworteinträge eingehen. Die Schlüsselableitungsfunktion MUSS ein anerkannt sicheres Verfahren mit ausreichender Iterationsanzahl im Einklang mit BSI TR-02102-1 nutzen.

Der Passwort-Manager DARF NICHT das Masterpasswort oder Informationen über das Masterpasswort (etwa Hashwerte) speichern beziehungsweise in der Datenbank ablegen.

APP.bd.8.A8 Sicherung der Passwörter (B)
Die Institution MUSS regeln, wie und wie häufig die Daten des Passwort-Managers gesichert werden. Die Daten des Passwort-Managers MÜSSEN entsprechend der Regelungen gesichert werden. Das Backup MUSS auch ohne Nutzung des Passwort-Managers lesbar sein (etwa Export als Textdatei für den Fall, dass die Datenbank defekt ist). Das Backup MUSS vor unberechtigten Zugriffen geschützt sein.

Es SOLLTE eine lokale Kopie der Passwortdatenbank auf einem separaten Gerät gesichert werden, um bei einem Ausfall des Gerätes oder der Verbindung zum Datenbankserver auf die Zugangsdaten zugreifen zu können.

APP.bd.8.A9 Aktualität des Passwort-Managers (B)
Der Passwort-Manager MUSS auf dem aktuellen Stand der Sicherheitsanforderungen sein. Die Verantwortlichkeiten für die Sicherstellung der Aktualität MÜSSEN innerhalb der Institution klar definiert sein.

Der Passwort-Manager MUSS regelmäßig auf vollständige Funktionalität geprüft werden.

Die Institution MUSS eine Verwaltung von Updates in einem Patchmanagement etablieren. Die Institution MUSS ein Schwachstellenmanagement für die Kennwortverwaltung einführen.

Es MÜSSEN vertrauenswürdige Updates aus zuverlässiger Quelle umgesetzt werden. Unsichere oder nicht vertrauenswürdige Änderungen innerhalb der Anwendung DÜRFEN NICHT angewendet werden.

Falls das End-of-Life der Anwendung erreicht ist, MUSS ein alternativer Passwort-Manager ausgewählt und bereitgestellt werden.

Falls der Anbieter des Passwort-Managers seine Dienste nicht mehr zur Verfügung stellt, MUSS die Kennwortverwaltung eine Export-Funktion bereitstellen, damit der Anwender weiterhin die Zugangsdaten nutzen kann.

APP.bd.8.A10 Absicherung von Multi-User-Systemen (B)
Falls mehrere Nutzende den Passwort-Manager verwenden, MUSS eine Verwaltung der Anwendenden erfolgen.

Die Verantwortlichkeiten für die Verwaltung der Nutzenden MÜSSEN klar definiert sein.

Höhere privilegierte Personen (z.B. Administrierende) DÜRFEN KEINEN Zugriff auf vertrauliche Daten anderer Nutzender erhalten.

Die Handlungen der Anwendenden MÜSSEN nachvollziehbar dokumentiert sein.

APP.bd.8.A11 Verwaltung von Sitzungen (B)
Es MUSS eine Sitzungsverwaltung durch den Passwort-Manager erfolgen. Die Sitzungsverwaltung MUSS den Kennworttresor nach einer kurzen Zeitspanne ohne Interaktion mit dem Nutzenden sperren, sodass eine erneute Authentifizierung erforderlich ist. Der Nutzende SOLLTE die Datenbank eigenständig sperren können.

Es MUSS eine Limitierung der Anmeldeversuche erfolgen, um Brute-Force-Angriffe auf die Anmeldung der Kennwortverwaltung zu verhindern. Es SOLLTE eine zunehmende Verzögerung bei zahlreichen Anmeldeversuchen stattfinden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.bd.8.A12 Einbindung in das Notfallmanagement (S)
Der Passwort-Manager SOLLTE in das Notfallmanagement der Institution integriert werden. Es SOLLTE, soweit erforderlich, geregelt sein, wie im Notfall auf die Passwörter zugegriffen werden kann.

APP.bd.8.A13 Mehr-Faktor-Authentifizierung (S)
Der Zugriff auf Passwörter SOLLTE durch eine Mehr-Faktor-Authentifizierung abgesichert werden. Die Mehr-Faktor-Authentifizierung SOLLTE NICHT vom Anwendenden deaktiviert werden können.

APP.bd.8.A14 Vier-Augen-Prinzip (S)
Bei der Nutzung geteilter Passwortdatenbanken SOLLTEN Änderungen nur nach der Freigabe einer weiteren autorisierten Person (Vier-Augen-Prinzip) freigegeben werden.

APP.bd.8.A15 Integritätsschutz des Passwort-Managers (S)
Die Integrität des gesamten Passwort-Managers als Anwendung SOLLTE geschützt werden, um Manipulationen zu entdecken, etwa durch Signaturen kritischer Komponenten und Daten.

APP.bd.8.A16 Aufzeichnung von Ereignissen (Logging) (S)
Ein Passwort-Manager mit mehreren Nutzenden SOLLTE alle Ereignisse (Anmeldungen, Änderungen, automatisches Ausfüllen, etc.) protokollieren. Die Datei SOLLTE keine sensiblen Informationen wie Passwörter enthalten. Die Daten SOLLTEN auf einem zentralen, abgesetzten Server gespeichert werden.

APP.bd.8.A17 Isolierung des Passwort-Managers (Sandboxing) (S)
Der Passwort-Manager SOLLTE vom restlichen System isoliert betrieben werden. Zugriffe von anderen Programmen auf die Kennwortverwaltung SOLLTEN überprüft werden.

APP.bd.8.A18 Sichere Wiederherstellung bei Verlust des Masterpasswortes (S)
Der Passwort-Manager SOLLTE Verfahren zur Wiederherstellung der Kennwortdatenbank bieten, um die Datenbank bei Verlust des Masterpassworts wiederherstellen zu können. Es MUSS sichergestellt sein, dass nur autorisierte Personen ohne Masterpasswort die Datenbank wiederherstellen können (insbesondere sind triviale oder leicht zu erratende Sicherheitsfragen zu vermeiden).

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.bd.8.A19 Bereitstellung einer Hochverfügbarkeitsarchitektur (H)
Bei nicht lokalen Passwort-Managern mit erhöhtem Schutzbedarf SOLLTEN Maßnahmen zur Erhaltung der Verfügbarkeit getroffen werden. Ein vollständiger Systemausfall SOLLTE durch die eingesetzte Architektur verhindert werden.

APP.bd.8.A20 Automatische Erkennung von Bedienungsfehlern durch den Passwort-Manager (H)
Der Passwort-Manager SOLLTE eine automatische Erkennung von kritischen Handlungen durch den Nutzenden (unsichere oder doppelte Passwörter, Deaktivierung von Sicherheitseinstellungen, Teilen von Passwörtern, fehlende Sperrung der Datenbank, etc.) bereitstellen.

Neu erstellte Passwörter SOLLTEN daraufhin überprüft werden, ob sie in bekannten Listen kompromittierter Kennwörter enthalten sind.

Der Nutzende SOLLTE bei einem fehlerhaften Verhalten gewarnt werden.

APP.bd.8.A21 Überwachung des Passwort-Managers (Monitoring) (H)
Die Institution SOLLTE alle Aktivitäten des Passwort-Managers überwachen. Auffällige Ereignisse SOLLTEN analysiert werden, um geeignete Gegenmaßnahmen treffen zu können.

4. Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den benutzerdefinierten Baustein APP.bd.8 *Passwort-Manager* finden sich unter anderem in folgenden Veröffentlichungen:

- Sean Oesch und Scott Ruoti:
  „That Was Then, This is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password-Managers", 2019.
- Andrés Fábrega et al.:
  „Exploiting Leakage in Password Managers via Injection Attacks", USENIX Security Symposium, 2024.
- Efstratios Chatzoglou et al.:
  „Keep Your Memory Dump Shut: Unveiling Data Leaks in Password Managers", 2024.
- Daniel Schougaard et al.:
  „Evaluation of Professional Cloud Password Management Tools", 2016.

5. Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden Elementaren Gefährdungen sind für den Baustein „Passwort-Manager" von Bedeutung:

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust

MATERNA

Kreuzreferenztabelle zu elementaren Gefährdungen

Kreuzreferenztabelle	G 0.9	G 0.11	G 0.14	G 0.15	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.45
A1 Planung des Einsatzes des Passwort-Managers						×		×						×	×							×
A2 Umsetzung von Richtlinien			×	×		×	×	×			×			×	×							
A3 Verschlüsselte Speicherung aller Daten auf Endgeräten			×		×		×				×					×			×		×	
A4 Absicherung der Kommunikation			×	×			×				×					×			×		×	
A5 Umsetzung des Zero-Knowledge-Prinzips			×	×			×				×					×			×		×	
A6 Sicheres Ausfüllen mit Interaktionen des Benutzenden			×				×												×		×	
A7 Sicheres Masterpasswort			×		×		×				×						×					
A8 Sicherung der Passwörter	×	×	×		×		×			×	×	×					×	×	×	×		×
A9 Aktualität des Passwort-Managers									×				×	×								
A10 Absicherung von Multi-User-Systemen			×				×			×	×					×	×	×				
A11 Verwaltung von Sitzungen			×		×		×				×						×	×	×	×		
A12 Einbindung in das Notfallmanagement							×				×	×							×	×		
A13 Mehr-Faktor-Authentifizierung			×		×		×		×	×	×					×		×				
A14 Vier-Augen-Prinzip							×			×						×	×	×				×
A15 Integritätsschutz des Passwort-Managers								×	×				×						×		×	
A16 Aufzeichnung von Ereignissen (Logging)									×	×	×	×				×	×	×	×			
A17 Isolierung des Passwort-Managers (Sandboxing)			×								×								×			
A18 Sichere Wiederherstellung bei Verlust des Masterpasswortes										×							×	×				×
A19 Bereitstellung einer Hochverfügbarkeitsarchitektur	×	×										×								×		×
A20 Automatische Erkennung von Bedienungsfehlern durch den Passwort-Manager							×										×					
A21 Überwachung des Passwort-Managers (Monitoring)		×					×		×	×	×	×	×			×		×	×	×	×	

Jannik Schonefeld ist Werkstudent im Bereich Cyber Security Consulting bei Materna und beschäftigt sich mit den Themen AI Security und Sicherheitsaspekten von Large Language Models (LLMs). Sein Fokus liegt auf der Analyse von Angriffen auf KI-Systeme sowie der Entwicklung von Maßnahmen zur Absicherung dieser Modelle.

Ihr Kontakt im #TeamMaterna

Jannik Schonefeld
Cyber Security Consulting
jannik.schonefeld@materna.group

So erreichen Sie uns:

Materna Information & Communications SE
Robert-Schuman-Straße 20, 44263 Dortmund
Tel.: +49 231 - 5599 - 00
E-Mail: marketing@materna.group
www.materna.de