Samen aanjagen van vernieuwing

Handreiking Wachtwoordkluis

Selectiecriteria en stappenplan implementatie

Auteur(s): Ed de Vries
Versie: 1.0
Datum: 26 februari 2025
Kenmerk: Handreiking Wachtwoordkluis

Inhoudsopgave

1 Inleiding

Sterke en unieke wachtwoorden zijn belangrijk om accounts en gegevens te beschermen tegen ongeautoriseerde toegang. Aanvallen zoals brute force en credential stuffing maken gebruik van zwakke of hergebruikte wachtwoorden om systemen te compromitteren. Door lange, complexe en unieke wachtwoorden te gebruiken, wordt het risico op dergelijke aanvallen aanzienlijk verminderd.

Het beheren van wachtwoorden vormt echter een uitdaging voor zowel individuele gebruikers als organisaties. Een wachtwoordkluis biedt een veilige oplossing door wachtwoorden en andere gevoelige informatie gecodeerd op te slaan en te beheren. Deze kluizen helpen bij het genereren en veilig bewaren van sterke wachtwoorden, waardoor het risico op beveiligingsincidenten afneemt en het handmatig onthouden of noteren van wachtwoorden niet meer nodig is. Daarnaast kunnen moderne wachtwoordkluizen ook andere vertrouwelijke gegevens opslaan, zoals multifactorauthenticatie (MFA) codes, passkeys en cryptografische sleutels, waardoor ze een cruciale rol spelen in een bredere beveiligingsstrategie.

Wachtwoordkluizen kunnen worden ingezet voor verschillende doelgroepen. Ze kunnen beschikbaar worden gesteld voor alle medewerkers binnen een organisatie, maar ook specifiek worden gebruikt door IT-beheerders, studenten of afdelingen met verhoogde beveiligingsbehoeften.

Er bestaan twee hoofdtypen wachtwoordkluizen: Software-as-a-Service (SaaS)-oplossingen en lokaal beheerde wachtwoordkluizen. SaaS-oplossingen worden extern gehost door een leverancier en bieden voordelen zoals automatische updates, integratie met andere cloudservices en toegang vanaf verschillende apparaten. Lokaal beheerde wachtwoordkluizen draaien binnen de IT-infrastructuur van een organisatie en geven volledige controle over gegevensopslag en beveiligingsmaatregelen, wat vooral geschikt is voor organisaties met strikte compliance-eisen.

Hoe selecteer je een goede wachtwoordkluis?
Deze handreiking biedt instellingen een objectief kader voor de selectie van een wachtwoordkluis die voldoet aan erkende beveiligingsstandaarden en best practices. Hierbij wordt aangesloten bij internationale normen zoals NIST 800-63B, CIS Controls en ISO/IEC 27001.

1.1 Doel

Het doel van deze handreiking is om duidelijke en toetsbare selectiecriteria te bieden waarmee de veiligheid, betrouwbaarheid en compliance van wachtwoordkluizen beoordeeld kunnen worden.

1.2 Reikwijdte

Deze handreiking is bedoeld voor IT-beheerders, security officers en beleidsmakers en richt zich op wachtwoordkluizen voor zowel individuele gebruikers als de instellingen. Specifieke producten of leveranciers worden niet behandeld; in plaats daarvan biedt dit document een objectief beoordelingskader.

1.3 Het belang van selectiecriteria

In verschillende onderzoeken naar de beveiliging van wachtwoordkluizen zijn verschillende kwetsbaarheden geïdentificeerd die van invloed kunnen zijn op de betrouwbaarheid van deze producten.

Een studie uit 2019 analyseerde dertien veelgebruikte wachtwoordkluizen en identificeerde risico's zoals ongecodeerde metadata en gevoeligheid voor clickjacking[1]. Een recenter onderzoek uit 2024 wees uit dat slechts een beperkt aantal wachtwoordkluizen wachtwoorden correct versleutelt in het werkgeheugen, wat nodig is om bescherming te bieden tegen geavanceerde aanvallen zoals Cold Boot Attacks[2]. Daarnaast worden regelmatig nieuwe kwetsbaarheden ontdekt, zoals lekken die toegang tot versleutelde gegevens mogelijk maken, of gegevens onbedoeld opslaan in tijdelijke bestanden.

Deze inzichten benadrukken het belang van strikte selectiecriteria[3].

[1] https://arxiv.org/abs/1908.03296

[2] https://arxiv.org/abs/2404.00423

[3] https://connect.geant.org/2020/10/26/7-quick-questions-about-password-managers

2 Selectiecriteria voor wachtwoordkluizen

Bij de keuze van een wachtwoordkluis is het advies om duidelijke en objectieve criteria te hanteren. De onderstaande selectiecriteria zijn gebaseerd op internationale beveiligingsstandaarden, marktanalyses en onafhankelijke onderzoeken. Hoewel het volgen van deze selectiecriteria de kans op kwetsbaarheden aanzienlijk verkleint, biedt geen enkele wachtwoordkluis absolute veiligheid. Regelmatige evaluatie en updates blijven noodzakelijk in een continu veranderend dreigingslandschap.

Voer altijd zelfstandig een onderzoek uit naar de best passende wachtwoordkluis voor jouw instelling op basis van functionele- en beveiligingseisen en -wensen. Vergelijk de verschillende oplossingen die op dat moment beschikbaar zijn in de markt[4].

2.1 Minimale vereisten

Een wachtwoordkluis moet minimaal aan de volgende eisen voldoen om een basisniveau van beveiliging en betrouwbaarheid te garanderen.

Gebruikersvriendelijkheid

- Intuïtieve en eenvoudig te gebruiken interface.
- Ondersteuning Nederlandse taal.
- Optioneel ook de mogelijkheid om een andere taal in te kunnen stellen.
- Ondersteuning voor automatisch invullen en opslaan van wachtwoorden.
- Duidelijke en eenvoudige instructie, ondersteuning en documentatie voor nieuwe gebruikers.
- Mogelijkheid tot synchronisatie tussen verschillende apparaten zonder ingewikkelde configuratie.

Encryptie

- Minimaal AES-256-bit versleuteling overeenkomstig NIST SP 800-75[5].
- Encryptiehiërarchie overeenkomstig FIPS 140-2, inclusief RSA-2048 voor asymmetrische encryptie.
- Hashing van wachtwoorden: PBKDF2, Argon2 of bcrypt.
- Encryptiesleutels mogen nooit toegankelijk zijn voor de dienstverlener / leverancier en moeten lokaal worden gegenereerd en opgeslagen.
- Wachtwoorden moeten ook in RAM (werkgeheugen) versleuteld zijn opgeslagen.
- Transparantie over encryptiemethoden, sleutelbeheer en implementatie daarvan moet geborgd zijn.

Beveiligde gegevensoverdracht

- Synchronisatie en communicatie tussen apparaten moet worden beveiligd met TLS 1.2 of hoger.

[4] Voorbeeld van productvergelijking:
https://docs.google.com/spreadsheets/d/1b2zEEU8_YPsgo3nY1BJ72qgLXteP7Yt0_mnlYJ8m0RI/edit?gid=1030171130#gid=1030171130

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

Identiteit en authenticatie

- Ondersteuning Multi-Factor Authenticatie (MFA) zoals Time-based One-Time Password (TOTP).
- Ondersteuning voor FIDO2 / WebAuthn-passkeys om inloggen zonder wachtwoorden mogelijk te maken.
- Single Sign-On (SSO) via SAML 2.0, OIDC.

Sessiebeheer en beveiliging

- Ondersteuning voor sessie time-out en actie bij inactiviteit (zoals automatische vergrendeling).
- Opties voor ontgrendelen met PIN en/of biometrie (vingerafdruk of gezichtsherkenning).
- Beveiliging tegen geautomatiseerd hacken (brute-force).
- Ingebouwde bescherming tegen het genereren van zwakke wachtwoorden.
- Ondersteuning voor het gebruik van een Software Bill of Materials (SBOM) om inzicht te bieden in de gebruikte componenten en kwetsbaarheden.
- Regelmatige en tijdige beveiligingsupdates ter bescherming tegen nieuwe dreigingen en kwetsbaarheden.

Data breach alerts

- Automatische meldingen bij gedetecteerde datalekken die wachtwoorden of andere gevoelige gegevens kunnen compromitteren.

Onafhankelijke beveiligingsaudit

- De leverancier van de wachtwoordkluis wordt periodiek beoordeeld door een onafhankelijke auditor om naleving van beveiligingsstandaarden te controleren.
- Auditrapporten moeten openbaar beschikbaar zijn.
- Voldoen aan ISO/IEC 27001 en/of ISAE 3000 / 3402 type II.

Privacybescherming en beperking gegevensverzameling

- De wachtwoordkluis voldoet aan de vereisten van de AVG.

Ondersteunde besturingssystemen, browsers en apparatuur

- De wachtwoordkluis moet beschikbaar zijn voor verschillende besturingssystemen (MacOS, Windows, Linux) en browsers (Chrome, Firefox, Edge en Safari) die nog gangbaar en actueel zijn binnen de officiële support life cycle.
- Geschikt voor gebruik op gangbare apparatuur als applicatie, app en/of webapp.

2.2 Gewenste functionaliteiten

Aanvullend op de minimale vereisten kunnen de onderstaande gewenste functionaliteiten de beveiliging en het gebruik van een wachtwoordkluis verbeteren.

Veilig delen en verzenden van wachtwoorden

- Beveiligde methode voor delen van wachtwoorden binnen teams en met externen.
- Mogelijkheid voor het aanmaken en beheren van een gedeelde wachtwoordkluis.

Controle op wachtwoordveiligheid

- Controle op dubbel gebruik van wachtwoorden.
- Controle op zwakke (complexiteit) van wachtwoorden.
- Controle op gecompromitteerde wachtwoorden (dark-web monitoring).

Beveiligde opslag

- Mogelijkheid voor het opslaan van gevoelige notities en creditcardgegevens.

Import- en exportmogelijkheden

- Ondersteuning voor veilige import en export van wachtwoorden en andere gegevens zonder risico op datalekken.

Auditmogelijkheden en logging

- Gedetailleerd activiteitenlogboek voor beheerders en gebruikers.
- SIEM-integratie voor centrale monitoring.

Zero-knowledge architectuur

- De leverancier kan geen toegang verkrijgen tot versleutelde gegevens, zelfs niet in uitzonderlijke situaties.

Veilige accountherstel

- Ondersteuning voor herstelmethoden zonder datalek-risico’s, zoals recovery-keys in plaats van e-mail gebaseerd herstel.

Uitgebreide beheerfunctionaliteiten

- Beheerders moeten wachtwoordbeleid kunnen afdwingen.
- Ondersteuning voor monitoring van zwakke en hergebruikte wachtwoorden.

3 Implementatie van wachtwoordkluizen

Een goede implementatie van een wachtwoordkluis is van belang om de beveiliging en het gebruiksgemak te borgen. Dit hoofdstuk beschrijft de verschillende implementatieopties, inclusief stand-alone en centraal beheerde wachtwoordkluizen, en de stappen voor een succesvolle invoering.

3.1 Stand-alone vs Centraal beheerd

Er zijn verschillende manieren om een wachtwoordmanager te implementeren, afhankelijk van de behoeften en infrastructuur van een instelling. De keuze tussen een stand-alone en een centraal beheerde wachtwoordkluis hangt af van factoren zoals beveiliging, beheerbaarheid en gebruiksgemak.

- **Stand-alone wachtwoordkluizen**
  Dit zijn individuele applicaties die door gebruikers lokaal worden beheerd. Ze bieden een hoge mate van autonomie, maar kunnen uitdagingen opleveren als het gaat om back-ups, synchronisatie en toegangsbeheer.

- **Centraal beheerde wachtwoordkluizen**
  Deze worden op organisatieniveau beheerd en bieden betere controle over wachtwoordbeleid, naleving en toegangsbeheer. Ze zijn ideaal voor instellingen waar een gestandaardiseerd beveiligingsbeleid vereist is.

Bij het kiezen van een wachtwoordkluis moet rekening worden gehouden met de schaalbaarheid, integratiemogelijkheden met bestaande systemen en het niveau van gebruikersondersteuning dat nodig is voor een veilige implementatie en gebruik.

Kenmerk	Stand-alone	Centraal beheerd
Kosten	Laag	Hoog
Beheer	Individueel	Centraal
Veiligheid	Afhankelijk van gebruiker	Beter controleerbaar
Gebruiksgemak	Hogere autonomie	Makkelijker te implementeren

Een centraal beheerde wachtwoordkluis biedt aanvullend nog voordelen zoals betere integratie met identity management-systemen, betere auditmogelijkheden en ondersteuning voor compliance.

3.2 PAM-oplossingen (Privileged Access Management)

Voor organisaties met hoge beveiligingseisen kan een PAM-oplossing een uitkomst zijn. PAM biedt extra bescherming voor beheerdersaccounts en systeemwachtwoorden door:

- Automatisch genereren en roteren van beheerderswachtwoorden.
- Het beperken van toegang op basis van tijd of rol.
- Uitgebreide logging en monitoring van sessies.
- Extra authenticatiestappen zoals MFA of hardwaretokens.

3.3 Stappenplan implementatie

Een gestructureerde implementatie zorgt ervoor dat gebruikers de wachtwoordkluis effectief en veilig kunnen gebruiken. Hieronder volgt een beknopt stappenplan om een succesvolle invoering te realiseren.

Stap 1: Onderzoek en selectie
Bepaal de behoeften en vereisten voor een wachtwoordkluis binnen de instelling. Vergelijk verschillende oplossingen op basis van beveiligingsvereisten, gebruiksgemak en integratiemogelijkheden. Zie hoofdstuk 2.

Stap 2: Beleid en richtlijnen opstellen
Ontwikkel interne beleidsregels en richtlijnen voor het gebruik van de wachtwoordkluis. Definieer regels over het gebruik, beheer, delen en beveiligen van wachtwoorden.

Stap 3: Training en bewustwording
Organiseer trainingen en bewustwordingscampagnes voor medewerkers en studenten. Zorg ervoor dat gebruikers begrijpen hoe de wachtwoordkluis werkt en waarom het belangrijk is om sterke wachtwoorden te gebruiken.

Stap 4: Technische implementatie
Installeer en configureer de wachtwoordkluis volgens de beveiligingsrichtlijnen. Integreer de oplossing met bestaande Identity & Access Management (IAM)-systemen en test de functionaliteit.

Stap 5: Monitoring en evaluatie
Implementeer monitoringtools om het gebruik en de veiligheid van de wachtwoordkluis te bewaken. Controleer regelmatig of de wachtwoordkluis voldoet aan de actuele beveiligingseisen en beleidsregels.

Stap 6: Ondersteuning en continue verbetering
Bied ondersteuning via een helpdesk en zorg voor regelmatige updates en verbeteringen. Houd gebruikers op de hoogte van nieuwe functionaliteiten en beveiligingsmaatregelen.