INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

Wachtwoordkluizen!

INFORMATIE
BEVEILIGINGS
DIENST

De gastheer van vandaag

VNG Realisatie

Jule Hintzbergen

INFORMATIE BEVEILIGINGS DIENST

Doel Webinar

VNG Realisatie

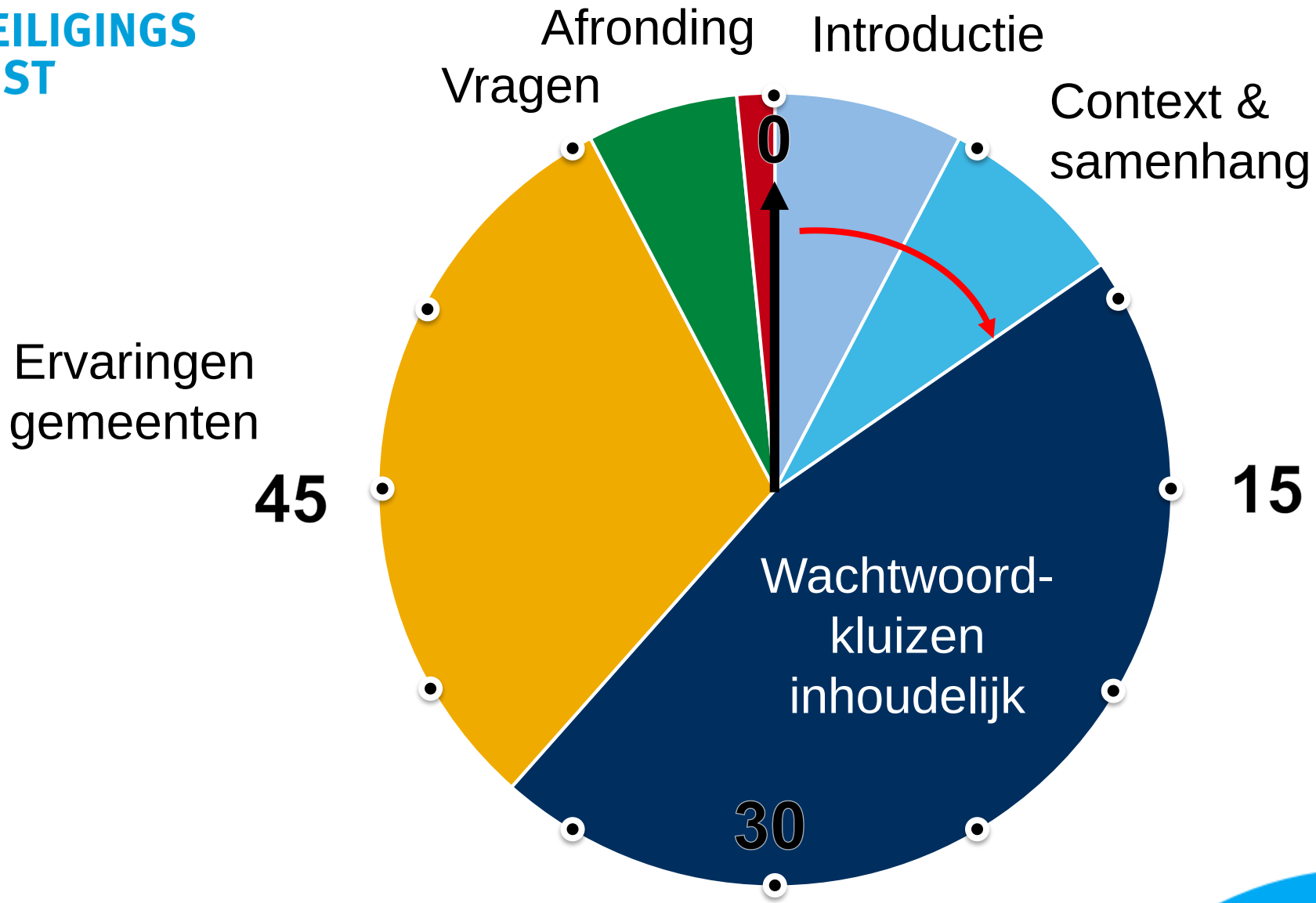
Na het volgen van deze webinar:

- Is er beter inzicht in de BIO eisen van wachtwoordkluizen
- Is er meer duidelijkheid over het onderwerp wachtwoordkluizen
- Is er kennis gedeeld, ook door andere deelnemers
- Kun je zelf aan de slag met wachtwoordkluizen

Webinar wachtwoordkluizen (60 min)

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie



INFORMATIE BEVEILIGINGS DIENST

Inhoud

VNG Realisatie

- Introductie
- Context & samenhang
- Wachtwoordkluizen
- Ervaringen
- Vragen
- Afronding

INFORMATIE BEVEILIGINGS DIENST

BIO Eisen

VNG Realisatie

9.3.1	1	**Geheime authenticatie-informatie gebruiken**		Secretaris/algemeen
9.3.1.1	9.4.3	1	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Dienstenleverancier
	9.4.3.1	1	Als er geen gebruik wordt gemaakt van two-factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	
	9.4.3.2	2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	
	9.4.3.3	2	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	
	9.4.3.4	2	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	
	9.4.3.5	2	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	

INFORMATIE BEVEILIGINGS DIENST

Waarom wachtwoordkluizen

VNG Realisatie

Problemen:

- Hergebruik van wachtwoorden
- Makkelijk onthoudbare reeksen
- Opschrijven van wachtwoorden
- Vergeten van wachtwoorden
- Stelen van wachtwoorden

Dus:

- Sterke wachtwoorden maken en kunnen onthouden
- De toename in wachtwoorden beheersen
- Voorkomen stelen van wachtwoorden door beveiligen
- Instellen unieke en sterke wachtwoorden voor iedere service of dienst
- Beheerders accounts apart en beter beveiligen

INFORMATIE BEVEILIGINGS DIENST

Wachtwoordkluizen

VNG Realisatie

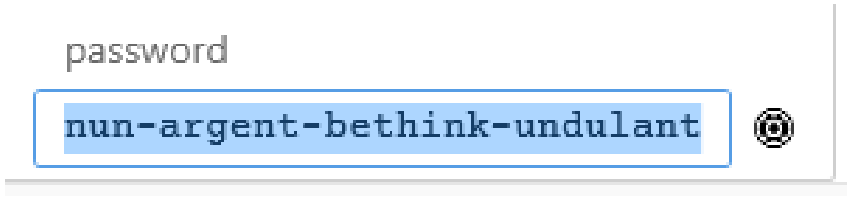
- Wachtwoordkluis is een programma met opslag voor wachtwoorden
- Toegang is afgeschermd met een wachtwoord
- Versleuteling van de opslag
- Versleuteling van transport
- Genereren wachtwoorden
- Opslag ook voor andere zaken, zoals notities,

INFORMATIE BEVEILIGINGS DIENST

Soorten

VNG Realisatie

Lokaal	Centraal
Lokale Applicatie	Server based, met een lokale applicatie
Soms in de browser	Centraal beheerd
Geen centraal beheer	Regels eenvoudig afdwingen
Backup zelf regelen	Logging
(synchronisatie)	Backup



INFORMATIE BEVEILIGINGS DIENST

Vormen - vervolg

VNG Realisatie

Stand alone (unmanaged):

- Gratis en betaald
- Voor diverse OS’en
- Speciale variant van de unmanaged: webbrowsers
- Voorbeeld Chrome

Centraal beheerd (managed):

- Kan ook stand alone zijn, met group policies (en decentrale opslag)
- Centrale opslag (ook cloud)
- Policies afdwingbaar

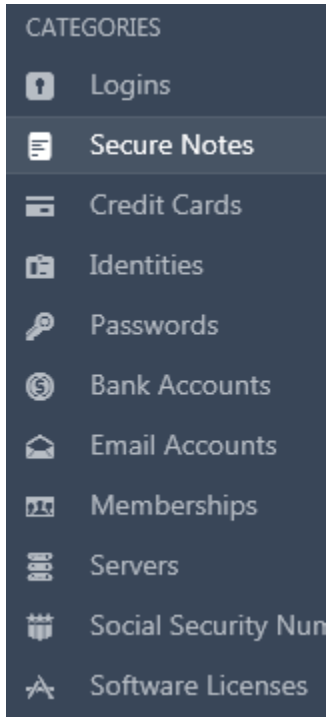
INFORMATIE BEVEILIGINGS DIENST

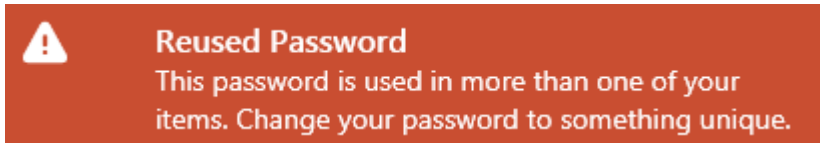
Aanvullende functionaliteit

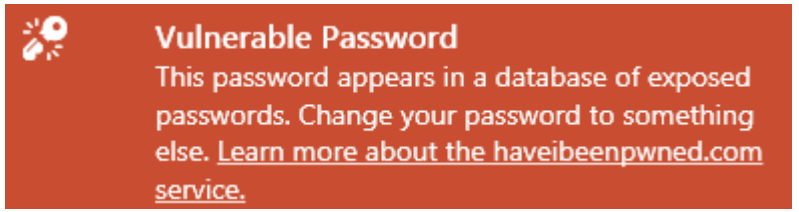
VNG Realisatie

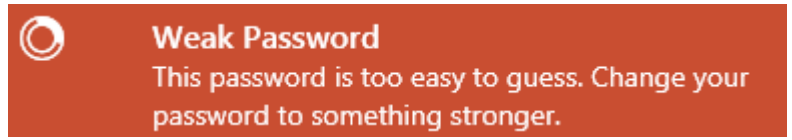
Wachtwoordkluizen hebben soms ook aanvullende functionaliteit:

- Sterke wachtwoord generatie
- Opslaan van notities
- Controle van wachtwoorden
- Waarschuwen voor hergebruik
- Waarschuwen voor “gevonden” wachtwoorden die jij ook gebruikt (dus: koppeling met haveibeenpwned)
- Een 2FA generator









INFORMATIE BEVEILIGINGS DIENST

Voordelen en nadelen

VNG Realisatie

	Standalone	Beheerd / Centraal
Voordelen	Snel in te zetten Lagere kosten Weinig beheer Geen post-its meer Wachtwoordgenerator Lagere beheerkosten op vergeten wachtwoorden	Auditeerbaar Compliancy Koppeling met centrale systemin (AD, Radius, LDAP) Integratie met IAM Centrale policies mogelijk 2FA toegang mogelijk (of FIDO) Meer en andere functionaliteit (PAM)
Nadelen	Minder goede beheersing Geen goed zicht op de plaats van opslag van de kluis Hogere beheerkosten door extra vragen Single point of failure Browserkluizen zijn vaak onveilig	Moeilijk uit te rollen Serieus project Beheerlast neemt toe Hogere kosten voor implementatie en beheer

(samenvatting van het document)

INFORMATIE BEVEILIGINGS DIENST

Risico's

VNG Realisatie

- Verliezen van het master wachtwoord
- Aanvallen op de wachtwoordkluis
  - Aanvallen op de host van de wachtwoordkluis
  - Aanvallen op geheugen (tijdelijke plaats van wachtwoorden)
- Zwak hoofdwachtwoord
- Fouten in de wachtwoordkluis (software fouten, clipboard hygiene, PIN)
- Foutief gedrag (autofill onderzoek)
- Sniffing (evil coffee shop attacker)
- Phishing attack
- Diverse vormen van sweep attacks (leeg trekken ww manager)
- Andere zwakheden (de aanvaller misbruikt een XSS injectie zwakheid)

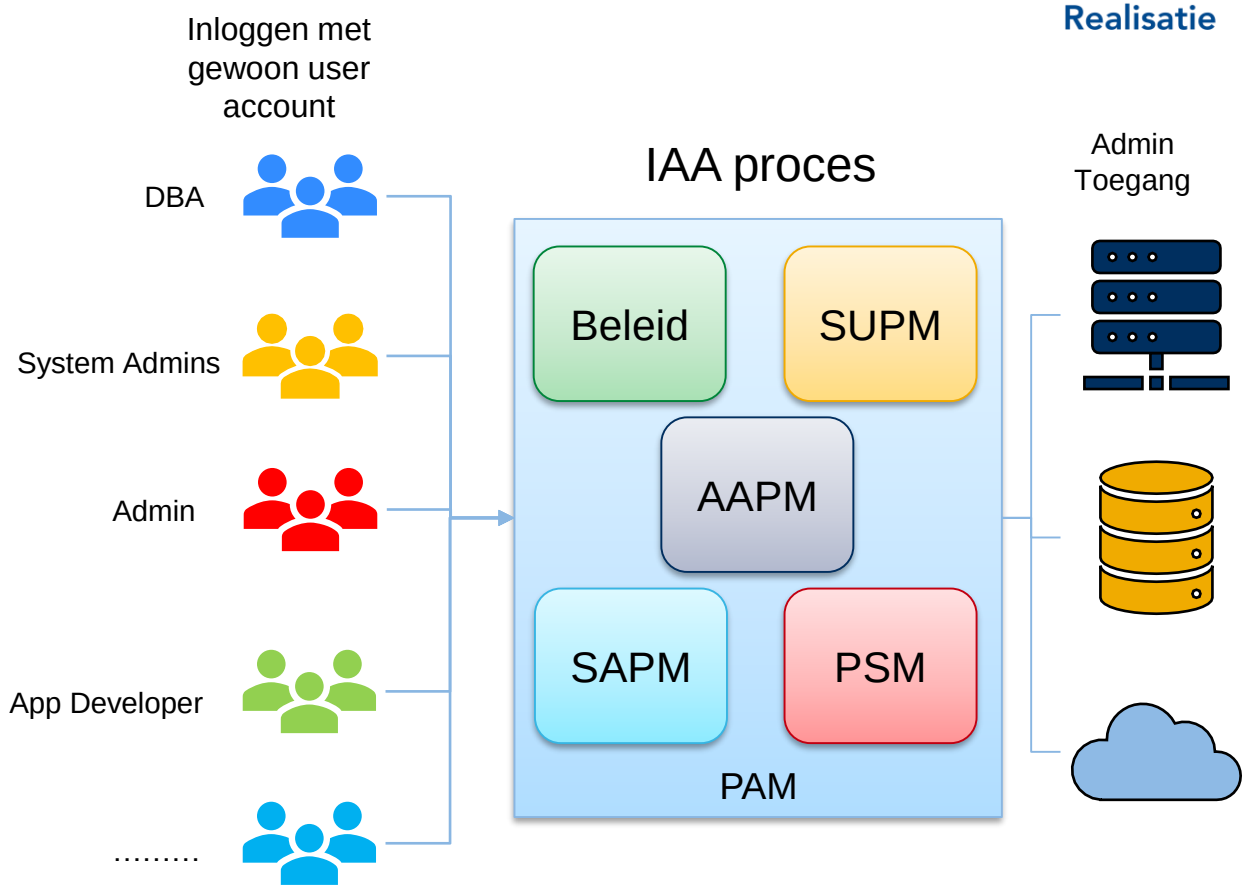
INFORMATIE BEVEILIGINGS DIENST

Wat nog meer

VNG Realisatie

PAM - Privileged Access Management

- SAPM – Shared Account/Access Management
- SUPM – Superuser Password Manager
- PSM - Privileged Session Management
- AAPM – Application to application Privileged Management / application Access Password Manager



INFORMATIE BEVEILIGINGS DIENST

Functionele eigenschappen

VNG Realisatie

1. Product ondersteunt de Nederlandse taal.
2. Multi-user/single user mogelijk
3. Audit trail mogelijk
4. Wachtwoord delen mogelijk
5. Ingebouwde authenticator voor 2FA
6. Ondersteunt BIO eisen
7. Met 2 - factor authenticatie inloggen in wachtwoordkluis
8. Browser-integratie, plug-ins voor meest gebruikte browsers beschikbaar.
9. Import / export mogelijk
10. Bevat een wachtwoordgenerator
11. Is het mogelijk om automatisch te checken of een wachtwoord al ergens anders voor gebruikt is

INFORMATIE BEVEILIGINGS DIENST

Niet functionele eigenschappen

VNG Realisatie

1. Moet passen bij de gemeenten en bruikbaar zijn met legacy.
2. Open Source
3. Cloud opslag
4. Lokale opslag mogelijk
5. Multiplatform
6. Sterke opslag versleuteling.
7. Sterke transport versleuteling (SSL/TLS).
8. Lage latency
9. Groeimodel mogelijk van standalone naar enterprise/managed.
10. De wachtwoordkluis beschikt over een hoofdwachtwoord herstel functie.

INFORMATIE BEVEILIGINGS DIENST

Hoe verder: Stappenplan voor de gemeente

VNG Realisatie

1. Stel een Business Case op (zie ook volgende slide).
2. Stel een programma van eisen (PvE) op.
   - functionele en niet-functionele eigenschappen (hoofdstuk 5)
3. Onderzoek welke wachtwoordkluis het beste past bij de gemeentelijke situatie.
   - op basis van het opgestelde PvE;
4. Stel beleid op voor het gebruik van wachtwoordkluizen binnen de gemeente.
   - voorbeeld beleid (bijlage 5);
5. Stel een handleiding op of gebruik de bijbehorende documentatie (als die er is);
6. Communiceer hierover naar alle medewerkers.
7. Distribueer de wachtwoordkluis software naar de gebruikers.
8. Monitor het gebruik van de wachtwoordkluis.

INFORMATIE BEVEILIGINGS DIENST

Business Case

VNG Realisatie

- Beschrijf een Business Case voor Wachtwoordkluizen?
  1. Luister naar de zorgen.
     - Wat zijn de zorgen met betrekking tot wachtwoordkluizen. Zorgen over budget, tijd, middelen of zelfs intern politiek?
  2. Deel gegevens.
     - Er zijn veel rapporten over het belang van wachtwoordbeveiliging en aanbevelingen voor het oplossen wachtwoord uitdagingen.
  3. Beschrijf alle voordelen.
  4. Bereken return on investment (ROI)
     - Kwantificeer productiviteitsverlies, bijvoorbeeld door het resetten van het account of doordat het account is geblokkeerd door te vaak het wachtwoord verkeerd in te typen.
  5. Et cetera.

INFORMATIE BEVEILIGINGS DIENST

Ervaringen gemeenten

VNG Realisatie

- Wie van jullie gebruikt er al wachtwoordkluizen?
  - Managed (centraal beheerd) of unmanaged (stand-alone)?
  - Hoe gekomen tot deze keuze?
    - Gebruik gemaakt van de Handreiking Wachtwoordkluizen?
    - Eventuele verbeterpunten.
  - Welke afwegingen hebben een rol gespeeld?
    - Zijn hierbij ook gebruikers betrokken? (Hoe ga je om met prive gebruik)
  - Gebruik gemaakt van een PvE?
    - Zou je die willen delen?
  - Welke communicatie hebben jullie ingezet om de medewerkers te infomeren / instrueren?
    - Zou je die willen delen?
- Wat zijn ervaringen van de gebruikers?
  - Voor- en nadelen
  - Knelpunten
- Wat kost het beheer?
  - T.o.v. voor het gebruik van wachtwoordkluizen.
  - Menskracht en financieel
  - Gestegen, gelijk of gedaald?
- Maakt iedereen binnen de gemeente gebruik van een wachtwoordkluis?
  - Of alleen beheerders of bepaalde afdelingen?
- Exit strategie?

INFORMATIE BEVEILIGINGS DIENST

Vragen

VNG Realisatie