Wachtwoord beleid

Informatieveiligheid & Privacy

SWO

Auteurs : Wilbert Hepping, Jan Lemstra

Versie : 1.0
Status : Definitief
Datum : 11 juli 2022

INHOUDSOPGAVE

Documenthistorie

Versie	Datum	Auteur(s)	Status / omschrijving wijziging
0.1	26-05-2021	Wilbert Hepping	Concept wachtwoordbeleid
0.2	10-06-2021	Wilbert Hepping	Aanpassing na overleg J. Lemstra
0.3	17-06-2022	Wilbert Hepping	Aanpassing in MFA / herauthenticatie
1.0	11-07-2022	Wilbert Hepping	Definitieve versie

Distributielijst

Naam	Organisatiedeel / Functie|Rol
Jan-Pieter Wind	FG
Daisy Djodikromo-de Jong	PO
Jan Lemstra	CISO
Johan Dijkink	Eenheidsmanager Advies en Services
Medewerkers SWO	Via Intranet

Review

Naam	Functie	Datum	Hoofdstukken/ onderwerpen

Accordering

Naam	Functie	Datum	Handtekening

1. Inleiding

Beleidsuitgangspunten voor het gebruik van wachtwoorden
Ten behoeve van de beveiliging van gegevens binnen de informatiesystemen van de gemeenten en Samenwerkingsorganisatie De Wolden Hoogeveen (hierna: SWO) is dit beleid er op gericht hoe met wachtwoorden omgegaan moet worden. Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder gemakkelijk toegang kunnen krijgen tot gegevens. Een gemakkelijk wachtwoord en onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit (juistheid, volledigheid en tijdigheid) van gemeentelijke informatie, maar uiteindelijk ook voor het imago van de organisatie. Alle gebruikers van onze informatiesystemen dienen zich te houden aan dit wachtwoordbeleid. Concreet betekent dat bijvoorbeeld dat men goede wachtwoorden moet kiezen en dat gebruikers verantwoordelijk zijn voor de geheimhouding van hun inloggegevens.

Het doel van dit wachtwoordbeleid is drieledig:

- Het vaststellen van regels waar wachtwoorden en wachtwoordprocedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.

De SWO hanteert de volgende beleidsuitgangspunten. Deze zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO) en de wereldwijd gehanteerde CIS Security baselines (Center of Internet Security).

Vanuit de BIO gaat dit over onderstaande controls en de daaraan gekoppelde de maatregelen.

H9. Toegangsbeveiliging
9.3.1: Geheime authenticatie-informatie gebruiken
9.4.1: Beperking toegang tot informatie
9.4.2: Beveiligde inlogprocedures
9.4.3: Systeem voor wachtwoordbeheer

Mochten de uitgangspunten tegenstrijdig zijn tussen de verschillende richtlijnen dan prevaleren de BIO controls en maatregelen.

2. Algemeen beleid

1. Standaard systeemwachtwoorden (wachtwoorden die standaard in software of hardware worden meegegeven), worden bij eerste ingebruikname direct gewijzigd.
2. Wachtwoorden worden nooit in originele, leesbare vorm ("plaintext") opgeslagen of verstuurd, maar in plaats daarvan in een versleutelde vorm opgeslagen (bijvoorbeeld de hashwaarde van het wachtwoord gecombineerd met een Salt).
3. Ten aanzien van wachtwoorden geldt:
   - Wachtwoorden worden op een veilige manier uitgegeven (bijvoorbeeld controle identiteit van de gebruiker)[1].
   - Tijdelijke wachtwoorden zijn maximaal 1 kalenderdag geldig en worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
   - Een door een gebruiker gewijzigd wachtwoord is minimaal 1 kalenderdag geldig om te voorkomen dat gebruikers door veelvuldig wijzigen direct kunnen terugkeren naar hun favoriete wachtwoord.
   - Een wachtwoord is alleen bij de gebruiker bekend.
   - Het aantal foutieve inlogpogingen staat op maximaal 3x, daarna wordt het account geblokkeerd. Hierna wordt het account minimaal 15 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker een verzoek indient deze lock-out op te heffen of het wachtwoord te resetten volgens de geldende procedure[2].
   - Binnen de organisatie wordt een zogenaamd "sterk wachtwoord beleid" gehanteerd. Dit betekent dat voor toegang tot informatiesystemen bepaalde eisen worden gesteld aan het wachtwoord. Met behulp van deze eisen wordt het achterhalen van een wachtwoord door onbevoegden vele malen lastiger. De volgende eisen worden aan het wachtwoord gesteld:
     - Als de applicatie of het systeem gebruikt maakt van multifactor authenticate (MFA) / Tweefactorauthenticatie (2FA)[3] dan mag een wachtwoord maximaal 1 jaar geldig zijn. In alle andere gevallen mag het wachtwoord maximaal 6 maanden worden gebruikt. Daarna moet een ander wachtwoord worden gekozen.
     - Een wachtwoord mag niet hetzelfde zijn als de voorgaande 10 wachtwoorden.
     - Het wachtwoord moet aan de volgende complexiteitseisen voldoen,
       1. Het wachtwoord mag niet de accountnaam van de gebruiker of een gedeelte met meer dan twee opeenvolgende tekens van de volledige naam van de gebruiker bevatten.
       2. Het wachtwoord moet ten minste 8 tekens lang zijn;
       3. Het wachtwoord moet tekens uit drie van de volgende vier categorieën bevatten:
          I. Hoofdletters (A tot en met Z)
          II. Kleine letters (a tot en met z)
          III. De cijfers 0 tot en met 9
          IV. Niet-alfabetische tekens (bijvoorbeeld !, @, $, # en %)

[1] Zie procedure verstrekken/wijzigen wachtwoorden
[2] Voor netwerkaccounts en applicaties met SSO volgens de 'Beslisboom wachtwoordreset door Servicedesk', voor overige accounts volgens de eigen procedure voor de betreffende applicatie.
[3] Zie H4. Multifactor authenticatie / Tweefactorauthenticatie.

Bij meer dan 20 karakters vervalt deze complexiteitseis.

4. Gebruikers behoren goede beveiligingsgewoonten in acht te nemen bij het kiezen en gebruiken van wachtwoorden. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:
   - Maak altijd gebruik van sterke wachtwoorden.
   - Wachtwoorden worden niet opgeschreven.
   - Gebruikers delen hun wachtwoord nooit met anderen.
   - Wachtwoorden mogen niet opeenvolgend zijn.
   - Gebruik verschillende wachtwoorden voor verschillende systemen/doelen, gebruik geen privé-wachtwoorden op het werk.
   - Geef nooit een wachtwoord op voor onderzoeken, vragen van anderen of om iemand te helpen. Het vragen om een wachtwoord moet worden aangemerkt als een veiligheidsincident. Dit dient te worden gemeld aan de binnen de organisatie vastgestelde persoon of organisatie;
   - Maak geen gebruik van de 'wachtwoord onthoud' functie van webbrowsers.
   - Maak geen gebruik van de functie om ingelogd te blijven.
   - Wachtwoorden moeten niet worden gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
   - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een ander.
   - Misbruik van wachtwoorden dient als beveiligingsincident gemeld te worden aan de servicedesk.
   - Maak gebruik van multifactor authenticatie (hierna: MFA) bestaande uit iets wat je weet (wachtwoord) en iets wat je hebt (mobiele telefoon, physical key, etc.), wanneer dit beschikbaar wordt gesteld.

3. Wachtwoordbeheer

3.1 Beheren en controleren van wachtwoorden binnen systemen/applicaties

Het beheren van wachtwoorden in systemen of applicaties behoort interactief te zijn en moet bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen conform de uitgangspunten uit dit wachtwoordbeleid. Op basis van dit beleid zijn de volgende concrete maatregelen voor het beheren / wijzigen van wachtwoorden in systemen of applicaties uitgewerkt.

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
2. Wachtwoorden hebben een geldigheidsduur zoals beschreven in dit beleid. Binnen deze termijn dient het wachtwoord te worden gewijzigd. Wanneer de termijn van een wachtwoord verlopen is, wordt het account automatisch geblokkeerd. Het is dan nog wel mogelijk het wachtwoord te wijzigen, zodat men weer toegang krijgt.
3. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende: Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthentiseerd (bijvoorbeeld door opnieuw in te loggen of via MFA).
4. Een gebruiker kan er zelf voor kiezen op elk willekeurig ander moment het wachtwoord te wijzigen.
5. De gebruiker is zelf verantwoordelijk voor het wijzigen of vrijgeven van het wachtwoord conform de voor de applicatie geldende procedure.

Wachtwoordbeleid dient zo veel als mogelijk binnen (informatie-)systemen te worden afgedwongen en indien mogelijk te worden gecontroleerd. De verantwoordelijkheid voor het uitvoeren van deze controle ligt bij de systeemeigenaar. De gevonden afwijkingen dienen te worden gerapporteerd aan de verantwoordelijk systeemeigenaar zodat maatregelen kunnen worden genomen om afwijkingen of fouten te herstellen.

3.2 Wachtwoordenkluis / wachtwoordmanager

Zoals beschreven in maatregel 9.3.1.1 van de BIO worden medewerkers door de SWO ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een vorm van een wachtwoordenkluis (ook wel wachtwoordmanager genoemd) waarmee de medewerker zijn of haar wachtwoorden kan beheren.

Een wachtwoordmanager is een applicatie om wachtwoorden te beheren. In de tool kunnen de huidige wachtwoorden worden opgeslagen, maar ook nieuwe “sterke” wachtwoorden aangemaakt worden. Om de tool te gebruiken hoeft de gebruiker vaak nog maar één wachtwoord te onthouden. Dit wachtwoord geeft toegang tot de opgeslagen wachtwoorden.

De toegang tot deze wachtwoordmanager is strict persoonlijk, er wordt gebruik gemaakt van tweefactorauthenticatie en een unlock-time na succesvolle authenticatie, dat wil zeggen dat de wachtwoordmanager na een bepaalde tijd weer op slot gaat.

Bij vertrek of rol/functie wijziging kan de toegang tot applicaties/informatie worden ontnomen of aangepast.

4. Multifactor authenticatie / Tweefactorauthenticatie

4.1 Wanneer Multifactor authenticatie / Tweefactorauthenticatie

Een normaal gebruikersaccount kent een gebruikersnaam en een wachtwoord. Dit noemen we vaak: "*iets wat je weet*". Tweefactorauthenticatie voegt daar een extra dimensie aan toe: "*iets wat je hebt*" of "*iets wat je bent*". In het eerste geval heeft men het dan over verschillende soorten tokens: USB token, een nummer generator of een sms code. In het tweede geval heeft men het dan over de biometrische kenmerken van een persoon. Gangbare varianten zijn: een vingerafdruk, een irisscan of je stem. Naast het wachtwoord wordt er dus om een extra verificatiemethode gevraagd.

Door tweefactorauthenticatie te gebruiken wordt het voor kwaadwillenden moeilijker om toegang te krijgen tot een account. Tweefactorauthenticatie geeft een extra zekerheid dat de persoon die inlogt ook daadwerkelijk diegene is die toegang mag hebben. Voor heel erg streng beveiligde systemen spreekt men soms ook nog van driefactorauthenticatie, in dit geval wordt gebruik gemaakt van iets wat je weet (wachtwoord, gebruikersnaam), iets wat je hebt (token of app op je smartphone) en iets wat je bent (biometrie).

Voor de beleidsregels met betrekking tot multifactor authenticatie passen we in ieder geval de Zero Trust[4] principes toe.

Binnen onze organisatie passen we multifactor authenticatie toe in de volgende gevallen:

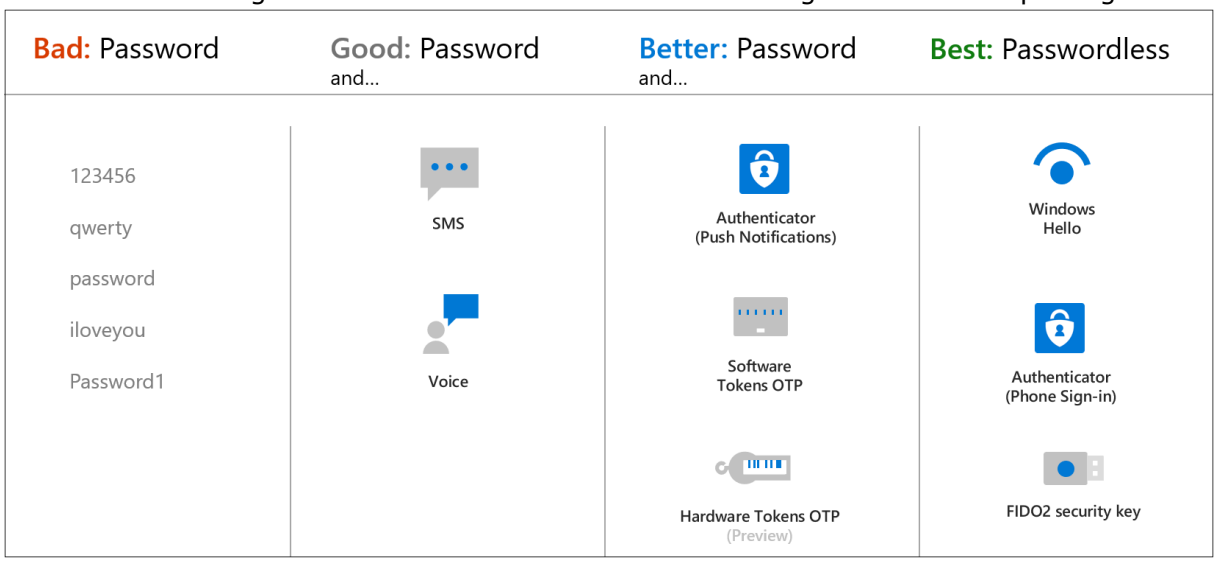
1. Toegang van buiten de (gemeentelijke) gebouwen tot de omgeving van de organisatie (van onvertrouwde zone naar vertrouwde zone);
2. Toegang van binnen de (gemeentelijke) gebouwen tot de netwerkomgeving (bijvoorbeeld Citrix omgeving en netwerkschijven);
3. Alle applicaties die rechtstreeks vanaf internet (van buiten de vertrouwde zone) te benaderen zijn (bijvoorbeeld Cloud/SaaS);
4. Alle systemen met persoonsgegevens, kritische toepassingen of toepassingen met een hoog belang;
5. Alle beheeraccounts van functioneel en technisch beheerders (intern en extern);
6. Alle mailomgevingen inclusief webmail en webapps (bijvoorbeeld Exchange, Outlook, overige e-mailaccounts);

4.2 Welke authenticatie- en verificatiemethoden worden toegestaan?

Onze organisatie wil op een zo veilig mogelijk manier MFA toepassen. Daarnaast zo min mogelijk verschillende MFA-toepassingen gebruiken om het voor de gebruikers zo eenvoudig mogelijk te maken.

[4] Zie Patchmanagement beleid SWO v1.0def.

In onderstaande figuur worden de verschillende methoden geclassificeerd op veiligheid.



Figuur 1: Aanbeveling Microsoft authenticatie concept[5]

Vanwege de vertrouwelijkheid van onze informatie wordt er gekozen voor een veiligheidsniveau van minimaal 'Better'. De organisatie zet hiervoor de MFA-toepassing van Azure AD in, in combinatie met de Authenticator app van Microsoft (Microsoft Authenticator) voor Push Notifications en OTP tokens.

Het gebruik van methode uit het veiligheidsniveau 'Good' (SMS en Voice) wordt afgeraden omdat deze methoden minder veilig zijn en zullen in de toekomst uitgefaseerd worden.

4.3 Hoe vaak herauthenticatie

De multifactor authenticatie (oftewel het inloggen met MFA) wordt per device opgeslagen in sessie waarin een zogenaamd 'sessiegeheim' wordt opgeslagen. De aard van een sessie is afhankelijk van de toepassing, bijvoorbeeld:

- Een webbrowsersessie met een 'sessie'-cookie;
- Een mobiele applicatie (app) die een sessiegeheim bewaart;

Sessiegeheimen moeten tijdelijk zijn. Dat wil zeggen, ze mogen niet oneindig worden bewaard. Periodieke herauthenticatie van sessies moet worden uitgevoerd om de aanwezigheid van de gebruiker bij een geverifieerde sessie te bevestigen. Voordat de sessie verloopt, kan de tijdslimiet voor herauthenticatie worden verlengd door de gebruiker te vragen naar één van de authenticatiemethode zoals eerder benoemd.

Wanneer een sessie is beëindigd vanwege een time-out of een andere actie (zoals het sluiten van de browser of het uitloggen door de gebruiker), moet de gebruiker een nieuwe sessie tot stand brengen door opnieuw te authenticeren.

Voor de maximale geldigheidsduur van een sessie volgen wij de NIST specificatie[6] voor verificatieniveau 1 (AAL1[7]). Deze schrijft een sessieduur van maximaal 30 dagen voor.

[5] Zie: https://docs.microsoft.com/nl-nl/azure/active-directory/authentication/concept-authentication-methods

De sessie moet worden beëindigd (d.w.z. uitgelogd) wanneer deze tijdslimiet is bereikt. Herauthenticatie kan gedaan worden door de gebruiker te vragen naar één van de authenticatiemethode zoals eerder benoemd.

[6] Zie: https://pages.nist.gov/800-63-3/sp800-63b.html
[7] Zie: https://docs.microsoft.com/nl-nl/azure/active-directory/standards/nist-about-authenticator-assurance-levels

5. Gehanteerde definities

Hashwaarde
Een hashwaarde is de uitkomst van een wiskundige berekening over de inhoud van een bestand en is altijd uniek. Een hashwaarde kan na berekening bijvoorbeeld een indicatie geven dat een bestand is veranderd zonder dat dit aan de uiterlijke kenmerken te zien is.

Salt
Bij 'salting', oftewel zouten, wordt willekeurige data toegevoegd aan een hashfunctie. Alsof het 'gezouten' wordt, vandaar de term. Het resultaat van de versleuteling van deze combinatie wordt opgeslagen. Data die gehasht is door een hashfunctie, is erg kwetsbaar voor een woordenlijstaanval.

Zero Trust
Voor uitleg Zero Trust zie Patchmanagement beleid SWO v1.0def.