Wachtwoordbeleid

Inhoudsopgave

Inleiding

Dit document geeft algemene aanwijzingen over het omgaan met wachtwoorden.

Het belang van correcte omgang met wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging van organisaties. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van informatie, maar uiteindelijk ook slecht voor het imago van de organisatie. Alle gebruikers van informatiesystemen dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en login-gegevens.

Wachtwoorden

2.1. Algemeen

Een wachtwoord is een reeks tekens waarmee toegang wordt verkregen tot informatie, een computer of een mobile device (smartphone, ipad etc.). Naast wachtwoorden wordt ook vaak de kans geboden om gebruik te maken van wachtwoordzinnen. Wachtwoordzinnen zijn meestal langer dan wachtwoorden met het oog op extra beveiliging en bevatten meerdere woorden die samen een zin vormen. Wachtwoordzinnen vragen vanwege hun lengte om veel meer ruimte in het invoervak of -veld. Wachtwoorden en wachtwoordzinnen helpen te voorkomen dat onbevoegde personen toegang krijgen tot bestanden, programma's en andere bronnen. Wanneer u een wachtwoord of wachtwoordzin maakt dan moet u deze sterk of lang maken. Dit betekent dat het wachtwoord of de wachtwoordzin moeilijk te raden of kraken is. Het is een goed idee om sterke wachtwoorden te gebruiken voor alle gebruikersaccounts op uw computer. Als u een bedrijfsnetwerk gebruikt, kan uw netwerkbeheerder van u eisen dat u een sterk wachtwoord gebruikt. Een wachtwoord behoort altijd te zijn toegewezen aan een gebruikersnaam, die een fysieke gebruiker uniek identificeert. Alle handelingen van een gebruiker moeten uniek kunnen worden toegewezen aan die gebruiker.

2.2. Eenmalige wachtwoorden versus statische wachtwoorden

Deze handleiding gaat over statische wachtwoorden, er bestaan echter ook nog eenmalige wachtwoorden (one time passwords). Een voorbeeld daarvan is het eenmalige wachtwoord dat gegenereerd kan worden door een token of door een applicatie. Denk aan google authenticator of een wachtwoord token dat steeds een nieuwe reeks cijfers of cijfers en letters genereerd. Dit laatste gebeurt dan op tijd of uit een bepaalde lijst.

2.3. Sterke en zwakke wachtwoorden

Wachtwoorden hebben een bepaalde sterkte nodig om het moeilijker te maken dat ze worden geraden. Dit kan door middel van bijvoorbeeld een brute force attack1 of door middel van bestaande wachtwoordlijsten (rainbow tables). De sterkte van een wachtwoord wordt bepaald door de lengte, de complexiteit en de onvoorspelbaarheid. Zwakke wachtwoorden zijn vaak te kort of een te eenvoudig woord of te eenvoudige toetsencombinatie.
Het gebruiken van een sterk wachtwoord reduceert het risico dat het wachtwoord kan worden geraden. Er zijn echter ook maatregelen nodig om de beveiliging, die verkregen kan worden door het gebruik van wachtwoorden, in stand te houden.

Deze aanvullende maatregelen zijn:

- Het vaststellen en implementeren van een beleid over wachtwoord gebruik binnen de organisatie, met daarin onder andere wachtwoord geldigheid.
- Het implementeren van goede wachtwoordprocessen voor verstrekken en resetten van wachtwoorden.
- De manier waarop in de applicaties wordt omgegaan met wachtwoorden.
- Medewerkers bewust maken dat wachtwoorden nooit gedeeld mogen worden.
- Wachtwoordsterktes technisch afdwingen.

Wachtwoordprocessen

Het verstrekken en wijzigen van geheime authenticatie-informatie (zoals bijv. wachtwoorden) dient met een formeel gestandaardiseerd proces te gebeuren. Bijvoorbeeld: er komt een medewerker in dienst, de manager vraagt een gebruikersaccount aan bij ICT (inclusief applicatie toegangsrechten), ICT maakt een nieuwe user aan en verstrekt het wachtwoord op een veilige manier aan de nieuwe gebruiker. Dit tijdelijke wachtwoord moet de eerste keer dat het wordt gebruikt direct worden gewijzigd en is maximaal een werkdag geldig. Denk hier

1 Uit Wikipedia: Brute force (Engels voor "brute kracht") is het gebruik van rekenkracht om een probleem op te lossen met een computer zonder gebruik te maken van algoritmen of heuristieken om de berekening te versnellen. Brute force wordt gebruikt als er geen algoritme bekend is dat sneller of efficiënter tot een oplossing leidt. De methode bestaat uit het botweg uitproberen van alle mogelijke opties, net zolang tot er een gevonden is die overeenkomt met de gewenste invoer.

ook aan een veilig wachtwoord wijzig proces voor het geval dat een medewerkers zijn of haar wachtwoord vergeten is, zowel voor computersystemen als voor applicaties.

Bij verandering van functie/afdeling of uitdiensttreding moeten ICT en de betrokken applicatiebeheerders ook in staat worden gesteld om tijdig rechten te kunnen veranderen en/of weg te nemen. Voor elke personeelsmutatie moeten ook de beheerders van applicaties in de Cloud of bij ketenpartners in staat worden gesteld om tijdig rechten te kunnen veranderen of weg te nemen.

Applicaties en wachtwoorden

Functioneel applicatiebeheerders kunnen voor al hun applicaties zelf gebruikers en wachtwoorden bijhouden in een tabel of gebruik maken van een centrale gebruikers database. In beide gevallen staat de gebruikersnaam en het wachtwoord in een tabel. In deze tabel mogen de wachtwoorden niet in klare (leesbare) taal staan. Standaard wordt van een wachtwoord een 'Hash' gemaakt en opgeslagen. Tevens moet men deze hashwaarde extra beschermen door het toevoegen van een getal, de zogenaamde 'Salt'2. Als een Salt wordt gebruikt is het voor een aanvaller die de wachtwoordtabel weet te bemachtigen zo goed als niet meer mogelijk de wachtwoorden terug te berekenen of de tabellen te gebruiken. Er zijn speciale hashing algoritmes ontworpen zoals Argon2 en PBKDF2 die het bruteforcen van wachtwoorden op basis van de hash zo moeilijk en tijdrovend mogelijk maken.

Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.

2.4. Risico's in relatie tot wachtwoorden

Risico's die niet direct te maken lijken te hebben met wachtwoorden maar dat wel zijn:
Afluisteren van het netwerk
Het versturen van wachtwoorden over onbeveiligde verbindingen (zoals http) is onveilig omdat de wachtwoorden kunnen worden uitgelezen. Als netwerkverkeer kan worden afgeluisterd kan ook de challenge response tussen systemen worden afgeluisterd. Daarmee kan informatie worden verkregen om wachtwoorden eenvoudig te raden en te gebruiken. Een tegenmaatregel kan zijn om gebruik te maken van encrypted verbindingen.

2 https://nl.wikipedia.org/wiki/Salt_%28cryptografie%29

Keyboard-loggers
Met een keyboard-logger wordt in dit geval een toetsenbord stekker bedoeld die tussen het toetsenbord en de PC wordt gestoken. Deze keyboard-loggers slaan alle toetsaanslagen op, en daarmee ook de ingetoetste gebruikersnamen en wachtwoorden. Er bestaan ook softwarematige keyboard-loggers. Een tegenmaatregel tegen fysieke keyboard-loggers is om regelmatig aan de buitenkant van de PC de toetsenbord aansluiting te controleren. De meeste antivirussoftware herkent de meeste softwarematige keyboard-loggers. Een maatregel tegen het risico van keyboard-loggers kan zijn om gebruik te maken van multifactor authenticatie.

Phishing
Bij phishing wordt gebruik gemaakt van een e-mail waarbij de eindgebruiker wordt verleid om zijn gebruikersgegevens, waaronder het wachtwoord, in te vullen op een malafide website. Tegenmaatregelen die kunnen helpen zijn: gebruik maken van een goede up-to-date antivirus scanner en er dient aandacht te zijn voor het openen van e-mailbijlagen in bewustwordingscursussen. Multifactor authenticatie helpt tegen phishing, mits de gebruiker niet verleid wordt om een eenmalig wachtwoord of tan-code af te geven.

Social engineering
Een social engineer zal proberen gebruikersgegevens te krijgen door zich bijvoorbeeld voor te doen als helpdeskmedewerker. Er wordt dus gewoon om wachtwoord en gebruikersgegevens gevraagd en vaak gekoppeld aan een probleem dat moet worden opgelost. Een tegenmaatregel tegen social engineering is dat het geaddresseerd moet zijn in bewustwordingscursussen.

Dumpster diving
Met dumpster diving wordt bedoeld dat iemand informatie verzameld door te zoeken in afval. Hier zit bijvoorbeeld informatie bij om een social engineering aanval uit te voeren. Een tegenmaatregel is dat voorkomen moet worden dat vuilnis makkelijk toegankelijk is en dat (gevoelige) informatie op papier wordt versnipperd/vernietigd.

Shoulder surfing
Meekijken met het invoeren van wachtwoorden. Een tegenmaatregel is dat men zich bewust moet zijn van deze vorm van een aanval en dat men het meekijken over de schouder voorkomt. Een andere tegenmaatregel is een privacy scherm bij de computer te gebruiken, dan wordt het in ieder geval moeilijker om mee te kijken op het scherm. Er bestaan ook oplossingen die het mogelijk maken om via biometrie in te loggen, hierdoor kunnen de inloggegevens niet over de schouder worden bekeken.

Software fouten
Door programmeerfouten in het schrijven van programma's kunnen er zwakheden worden geintroduceerd waardoor bijv. wachtwoorden makkelijk te achterhalen zijn. Wachtwoorden die niet of met een zwak algoritme worden gesalt, kunnen eenvoudiger gekraakt worden waardoor de wachtwoorden zichtbaar worden.. Een ander voorbeeld van een fout is dat webapplicaties gevoelig kunnen zijn voor SQL injectie aanvallen. Hierdoor kunnen bijvoorbeeld gebruikersnamen en wachtwoorden worden gelezen uit een tabel van de database, die bij de website hoort. Een tegenmaatregel kan zijn dat men software kwaliteitsprocessen invoert/handhaaft en software test voordat het in gebruik genomen wordt, door bijvoorbeeld een Pentest.

Opschrijven van wachtwoorden
Wachtwoorden worden soms op briefjes opgeschreven en aan de monitor geplakt, of onder het toetsenbord of op een andere onveilige plaats bewaard. Dit dient geaddresseerd te worden in bewustwordingscursussen. Een goed alternatief is het gebruikmaken van een wachtwoordmanager.

Gecompromitteerde database
Regelmatig komt het voor dat er op internet gebruikersnamen en wachtwoorden worden gepubliceerd. Dit zijn gegevens uit gecompromitteerde databases. Het kan bijvoorbeeld zijn dat er een e-mailadres in de database aanwezig is. Tegenmaatregelen kunnen zijn: regelmatig het wachtwoord wijzigen, andere wachtwoorden kiezen dan voor privé doeleinden, gebruik maken van tweefactorauthenticatie of van een eenmalige wachtwoord generator en

e-mailadressen van de organisatie alleen gebruiken voor zakelijke registraties op internet. Er zijn online websites te vinden die kunnen verieferen of het account door een hack openbaar beschikbaar zijn[3].

2.5 Hoe kiest men sterke wachtwoorden

Sterke wachtwoorden zijn doorgaans niet zo gemakkelijk om te onthouden. Het is daarom beter om een wachtwoordzin te gebruiken die wel voor de gebruiker betekenis heeft. Als algemene regel geldt dat wachtwoordzinnen op grond van hun lengte veiliger zijn dan zogenaamd 'sterke' (complexe) wachtwoorden. Deze zin kan bijvoorbeeld de eerste regel uit een boek zijn. Hoe gaat dit in zijn werk:

Neem een zin die u kunt onthouden.
Neem van ieder woord de eerste letter.
Bijvoorbeeld: 'Onze gemeente is een veilige organisatie in 2019' wordt dan
OGIEVOI2019. Als dan ook nog letters vervangen worden door leestekens en hoofd- en kleine letters worden gemixt ontstaat een erg moeilijk te kraken wachtwoord dat toch onthouden kan worden, het resultaat is dan: Og=€V0!2o19.
Indien toegestaan kan ook de gehele zin ingevoerd worden.

Indien er geen gebruikt wordt gemaakt van twee-factor authenticatie dient de wachtwoordlengte minimaal 8 posities en complex van samenstelling te zijn. Als een wachtwoord minimaal 20 posities lang is dan vervalt de complexiteitseis.

2.6. Wachtwoord gedragsregels

Algemeen

- Gebruik verschillende wachtwoorden voor verschillende systemen/doelen, gebruik geen privé-wachtwoorden op het werk.
- Gebruik verschillende wachtwoorden voor verschillende applicaties op het werk, minimaal voor de essentiële systemen die meer gevoelige informatie bevatten.
- Gebruik voor essentiële systemen een sterk wachtwoord en wissel dit regelmatig.
- Geef wachtwoorden aan niemand.
- Wachtwoorden mogen niet worden opgeschreven.
- Geef geen wachtwoorden door via e-mail, chat of andere elektronische communicatie en als dat toch moet, dan gescheiden (via een andere weg) van de gebruikersnaam.
- Geef geen al te gemakkelijke hints of controlevraag over het wachtwoord, bijvoorbeeld je naam of de meisjesnaam van je moeder.
- 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.
- Maak geen gebruik van de 'wachtwoord onthoud' functie van sommige webbrowsers.
- Maak geen gebruik van de functie om ingelogd te blijven.
- Maak altijd gebruik van sterke wachtwoorden.
- Wijzig een wachtwoord direct bij vermoeden van misbruik.
- Wachtwoorden moeten niet worden gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
- Bij een grote hoeveelheid logins en wachtwoorden is het aan te bevelen om deze op te slaan in een daarvoor bedoelde veilige applicatie of app, zie: wachtwoordmanagers.

Aanwijzingen voor applicaties en applicatie ontwikkeling

- Wachtwoorden worden uitsluitend gebruikt voor natuurlijke en unieke aanwijsbare personen, en systemen indien mogelijk moet het gebruik van groepsaccounts worden vermeden.
- Wachtwoorden mogen niet in klare (leesbare) taal of ongezouten (Un Salted) worden opgeslagen.

3 https://haveibeenpwned.com/

- Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.

2.7. Wachtwoordmanagers

Wachtwoordmanagers worden steeds vaker gebruikt. Een wachtwoordmanager is een tool 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 maar één wachtwoord te onthouden. Dit wachtwoord geeft toegang tot de opgeslagen wachtwoorden. Er zijn twee categorieën wachtwoordmanagers: centraal beheerd en stand-alone (online en offline varianten). Zakelijk gezien kan het gebruik van een centraal beheerde wachtwoordmanager nog meer voordelen opleveren omdat ook bij vertrek of rol/functie wijziging gelijk de toegang tot applicaties/informatie kan worden ontnomen of aangepast. Ook kunnen wachtwoordregels per applicatie/toegang beter afgedwongen worden en doorgaans audit proof gelogd worden. Wachtwoordmanagers worden bij voorkeur gebruikt met tweefactorauthenticatie en een unlock-time na succesvolle authenticatie, dat wil zeggen dat de wachtwoordmanager na een bepaalde tijd weer op slot gaat. Een wachtwoordkluis dient beschikbaar gesteld te worden aan de medewerkers.

2.8. Multifactor authenticatie

Een normaal gebruikersaccount kent een gebruikersnaam en een wachtwoord, dit noemen we vaak: “iets wat je weet”. Tweefactorauthenticatie[4] 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, een sms code. In het tweede geval heeft men het dan over de biometrische kenmerken van een persoon, de meest gangbare zijn: een vingerafdruk, een irisscan of je stem. Naast het wachtwoord wordt er 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 3-factor authenticatie, in dit geval wordt gebruik gemaakt van iets wat je weet (wachtwoord, gebruikersnaam), iets wat je hebt (token) en iets wat je bent (biometrie). In situaties waar geen twee-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1).

2.9. Controle van wachtwoorden

Wachtwoordbeleid dient zo veel als mogelijk binnen (informatie-)systemen te worden afgedwongen en indien mogelijk te worden gecontroleerd. De controle en de gevonden afwijkingen dienen te worden gerapporteerd aan het management zodat maatregelen kunnen worden genomen om fouten te herstellen. Voor (informatie)-systemen die voldoen aan het wachtwoordbeleid geldt een maximale geldigheidsduur van een jaar en daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.

4 https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/

Bijlage 1: Wachtwoordbeleid

Beleidsuitgangspunten voor het gebruik van wachtwoorden

Ten behoeve van de beveiliging van informatie binnen systemen van de organisatie is dit beleid er op gericht hoe met wachtwoorden omgegaan moet worden. Wachtwoorden vormen een belangrijk aspect van informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie van de organisatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit van informatie, maar uiteindelijk ook voor het imago van de organisatie. Alle gebruikers van informatiesystemen van de organisatie dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en 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.

Algemeen beleid

1. Standaard wachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd.

2. Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord gecombineerd met een Salt opgeslagen.

   Ten aanzien van wachtwoorden geldt:
   - Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
   - Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord. Tijdelijke wachtwoorden zijn maximaal een werkdag geldig.
   - Gebruikers bevestigen de ontvangst van een wachtwoord.
   - Wachtwoorden zijn alleen bij de gebruiker bekend.
   - Zonder twee-factor authenticatie dienen wachtwoorden te bestaan uit minimaal 8 vrij te kiezen karakters en complex. Bij meer dan 20 karakters vervalt de complexiteitseis.
   - Wachtwoorden zijn maximaal een jaar geldig indien de (informatie)-systemen voldoen aan het wachtwoord beleid. Anders zijn de wachtwoorden maximaal 6 maanden geldig.
   - Het aantal foutive inlogpogingen staat op maximaal 10x, daarna wordt het account inactief.

   Gebruikers behoren goede beveiligingsgewoonten in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

3. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:

   - Wachtwoorden worden niet opgeschreven.
   - Gebruikers delen hun wachtwoord nooit met anderen.
   - Wachtwoorden mogen niet opeenvolgend zijn.
   - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
   - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
   - Misbruik van wachtwoorden dient als beveiligingsincident gemeld te worden aan de servicedesk.
   - Nadat voor een gebruikersnaam drie keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 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.

Aanvullend beleid voor wachtwoorden van systeembeheerders

Toegang tot besturingssystemen van de organisatie behoort te worden beheerst met een beveiligde inlogprocedure.

1. Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.[5]

2. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.

3. Voorafgaand aan het aanmelden van een kritische applicatie wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.

4. Bij een succesvol loginproces van een kritische applicatie wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.

5. Voor mobiele apparaten wordt de Wipe functie geactiveerd bij vaker dan 5 maal[6] foutief inloggen.

6. Wachtwoordbeheer

   Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

   1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).

5 Met twee-factor authenticatie wordt bedoelt : iets dat je weet (je wachtwoord) en iets dat je hebt (bijvoorbeeld een fysieke/soft token, key generator of vingerafdruk).

6 Zelf aanpassen naar wat gebruikelijk is binnen de gemeente op basis van een risicoinschatting.

2. Wachtwoorden hebben een geldigheidsduur. Binnendeze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.

3. Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een geldigheidsduur van maximaal een dag en moeten bij het eerste gebruik worden gewijzigd.

4. 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 geauthenticeerd.

[Naam. Functie] [Naam. Functie]

_____ _____

Dit document is gebaseerd op de handreiking 'Wachtwoordbeleid BIO' van de informatiebeveiligingsdienst. Bron: "Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten", licentie onder: CC BY-NC-SA 4.0.

Bezoek http://creativecommons.org/licenses/by-nc-sa/4.0 voor meer informatie over de licentie.