Wachtwoordcomplexiteit

Vanaf versie 1.12 zijn de eisen die gesteld worden aan een nieuw wachtwoord veranderd. Dit is in overeenstemming met de toentertijdse inzichten met betrekking tot sterke wachtwoorden, zoals onder andere verwoord in de nieuwste standaard van het NIST (800-63-3B). Hierbij wordt minder waarde gehecht aan het vaak veranderen van een wachtwoord, en het gebruik van hoofdletters en speciale tekens omdat dit contraproductief werkt. Het gaat erom dat een wachtwoord moeilijk voorspelbaar is. De nieuwe wachtwoordeisen beoordeelt een nieuwe wachtwoord daarom onder meer op lijsten veel gebruikte wachtwoorden, toetsenbord- en tekenreeksen, woordenboekwoorden en dergelijke. De vereiste kwaliteit kan door de beheerder naar wens verhoogd worden. Zie *Item: minimumwachtwoordcomplexiteit* bij: Sectie Logon.

Naast de controle op complexiteit wordt onder andere gecontroleerd op minimum lengte. Zie lemma Inloggen.

Natuurlijk is het ook aan de gebruiker om het wachtwoord vervolgens geheim te houden. Gebruik het wachtwoord dan ook niet in andere applicaties die niet onder het beheer van dezelfde organisatie vallen. Daarnaast is het gebruik van 2-factor authenticatie een essentieel onderdeel van de beveiliging van publiek toegankelijke webapplicaties.

Inloggen