/// Wachtwoordbeleid

1 INTRODUCTIE

Een wachtwoordbeleid is de basis van elke organisatie haar authenticatie-omgeving. Het omschrijft duidelijke richtlijnen met betrekking tot wachtwoorden en wachtwoordprocedures. De Vlaamse overheid beschouwt bijvoorbeeld alleen het gebruik van wachtwoorden om toegang te krijgen tot informatie en systemen als een zwak identificatiemiddel. Daarom raadt de Vlaamse overheid aan om maximaal in te zetten op multifactor-authenticatie (MFA) als onderdeel van uw wachtwoordprocedures.

Multifactor-authenticatie (MFA) bestaat uit meerdere factoren om toegang te verkrijgen tot informatie en systemen, waarbij wachtwoorden één van deze factoren kunnen zijn. Hoewel multifactor-authenticatie (MFA) uit meerdere factoren bestaat om toegang te krijgen, bestaat de kans altijd dat één van deze factoren faalt.

Het is daarom belangrijk om binnen uw organisatie een sterk wachtwoordbeleid te hanteren. Om een succesvol beleid te implementeren is het ook belangrijk dat het toezicht erop wordt toegewezen aan een beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en de bevoegdheid om de toepassing en naleving van het beleid op te volgen en eventuele inbreuken hiervan te rapporteren.

2 WET- EN REGELGEVING

Lokale besturen staan volgens de Belgische en Europese regelgeving vrij om hun wachtwoordbeleid, en wachtwoordparameters te configureren naar eigen behoeften.

Echter, lokale besturen dienen wel rekening te houden met de Algemene Verordening Gegevensbescherming (AVG) of GDPR (General Data Protection Regulation)[1]. Deze regelgeving schrijft voor dat alle bedrijven, overheidsdiensten, organisatie en instellingen die in Europa persoonsgegevens verwerken, gebruiken, registreren of bewaren, moeten voldoen aan bepaalde richtlijnen. Deze richtlijnen stellen dat gegevens volgens een afdoend veiligheidsniveau moeten worden verwerkt binnen een organisatie. Met andere woorden, om te voldoen aan de AVG, wordt er verwacht dat persoonsgegevens niet zomaar door iedereen ingezien kunnen worden, en dus onder andere versleuteld zijn met een wachtwoord.

De Vlaamse overheid beveelt de volgende configuratie van de wachtwoordparameters aan:

- Een minimumlengte voor wachtwoorden van 14 karakters (of het gebruik van wachtwoordzinnen).
- Afdwingen van complexiteitseisen.
- Een maximum wachtwoordleeftijd van 90 dagen.
- Een minimaal wachtwoordleeftijd van 1 dag.
- Een wachtwoordgeschiedenis van 24 vorige wachtwoorden.
- Account lock-out na 5 mislukte inlogpogingen in 30 minuten.

3 BELEID

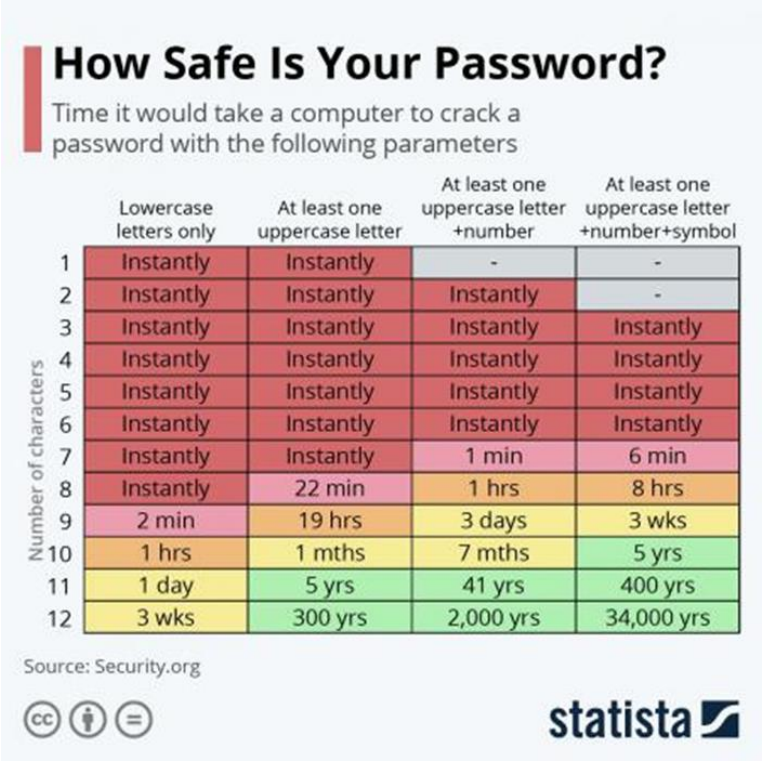
Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot wachtwoordbeheer. Bij het inrichten van wachtwoordprocedures is het belangrijk om te bepalen welke informatie ingezien kan worden bij een correcte wachtwoordauthenticatie. Op basis van de informatieklassebepaling[2] kan er bijvoorbeeld gekozen worden om multifactor-authenticatie in een wachtwoordprocedure te integreren. Bijkomend is het belangrijk om de juistheid en continuïteit van gedefinieerde wachtwoordprocedures en wachtwoordparameters te monitoren, rapporteren en op te volgen.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot de verschillende wachtwoordprocessen en wachtwoordparameters beschreven staan. Het is belangrijk om wachtwoordprocedures en wachtwoordparameters te veranderen wanneer er aanwijzingen zijn van non-compliance of nieuwe aanvalsvectoren.

Onderstaande tabel toont aan dat hoe sterker je wachtwoord is, hoe moeilijker het is om dit te kraken.



Mensgerichte maatregelen

Mensgerichte maatregelen verwijzen naar het hebben van bewustmakingscampagnes die het belang van een gedegen wachtwoordbeheer benadrukken bij gebruikers en applicatiebeheerders. Dergelijke campagnes zullen ervoor zorgen dat de beleidsprocedures en processen daadwerkelijk gedragen zullen worden door al uw medewerkers en partners.

4 AANBEVELINGEN

Organisatorische maatregelen

- Zorg ervoor dat de verantwoordelijkheden voor het implementeren en onderhouden van het wachtwoordbeheer processen en procedures goed gedefinieerd en bekend zijn.
- Zorg ervoor dat wachtwoordrecovery en wachtwoordverandering procedures gebruik maken van multifactor-authenticatie.
- Definieer voor het wachtwoordbeheer KPIs, en monitor en review deze op geplande tijdstippen.
- Voer regelmatig een audit uit die uw wachtwoordbeheer controleert

Technische maatregelen

- Volg de wachtwoordparameters van de Vlaamse Overheid:
    - Een minimumlengte voor wachtwoorden van 14 karakters (of het gebruik van wachtwoordzinnen).
    - Afdwingen van complexiteitseisen.
    - Een maximum wachtwoordleeftijd van 90 dagen.
    - Een minimaal wachtwoordleeftijd van 1 dag.
    - Een wachtwoordgeschiedenis van 24 vorige wachtwoorden.
    - Account lock-out na 5 mislukte inlogpogingen in 30 minuten.

- Monitor gefaalde loginpogingen en rapporteer verdacht gedrag

Mensgerichte maatregelen

- Voer interne phishing-campagnes uit om de bewustwording bij medewerkers en beheerders te vergroten.
- Schrijf het gebruik van een wachtwoordmanager voor.
- Sensibiliseer medewerkers en beheerders over het belang van wachtwoordbeheer door middel van bestaande documentatie.
- Zorg ervoor dat in de onboarding van nieuwe medewerkers, het belang van wachtwoordbeheer benadrukt wordt.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
MFA	Multifactor-authenticatie is een elektronische authenticatie-methode waarbij gebruikers pas toegang krijgen tot een website of applicatie nadat gebruikers zich twee (of meer) keer geauthenticeerd hebben.	Toegangsbeheer | Vlaanderen.be

REFERENTIES

- Informatieveiligheid Wachtwoorden Vlaamse overheid:
  Wachtwoorden | Vlaanderen Intern
- Informatieveiligheid Wachtwoorden Vlaamse overheid sensibilisering:
  Behandel je wachtwoorden zoals je onderbroeken | Vlaanderen Intern