Wachtwoord beleid VSBfonds advies document

Inleiding
Met de nabije overgang van AV naar Dynamics, is het belangrijk dat VSBfonds op het gebied van IT, goed voorbereid is. VSBfonds heeft een IT Audit gehad met Mark Schotsman van BDO, om te informeren over de eisen waaraan wij moeten voldoen, om succesvol door de jaarrekening controle bij BDO heen te komen. In het gesprek, zijn we er o.a. achter gekomen dat er geen duidelijke regels zijn, omtrent het gebruik/handelen van wachtwoorden binnen VSBfonds.

In dit document zal er een advies worden geschreven, over de wijze waarop VSBfonds in het Dynamics tijdperk verder kan en daarmee een positieve beoordeling krijgt van BDO op het gebied van wachtwoorden.

Analyse
VSBfonds werkt momenteel met een *"create and forget"* methode voor het maken van wachtwoorden. Dit houdt in, dat er bij het aanmaken van een nieuwe gebruiker, een wachtwoord wordt aangemaakt die niet meer wordt gewijzigd (tenzij gevraagd/kwijt).
Zo kunnen wachtwoorden een enorm lange periode hetzelfde blijven en is er potentieel een gevaar voor inbreuk binnen het systeem. Dit kan gevaarlijk zijn omdat wachtwoorden op meerdere wijze gekraakt kunnen worden:

- door meekijken tijdens het invoer van het wachtwoord (het zogeheten "shoulder surfing").
- door het delen van het wachtwoord (bijvoorbeeld tijdens afwezigheid/vakantie).
- door het stelen van het wachtwoord van de plek waar het is genoteerd (bijvoorbeeld op een post-it, in de agenda of in een tekstbestand op de computer)
- door het wachtwoord af te luisteren tijdens de communicatie met het IT object (bijvoorbeeld invoer op een website)
- door een wachtwoord met meerdere pogingen te raden tijdens aanmelden.
- door het wachtwoord te raden/kraken van een (ongeautoriseerd) verkregen wachtwoordhash, een versleutelde versie van een opgeslagen wachtwoord (bijvoorbeeld verkregen uit een datalek).

Momenteel wordt er al het e.e.a. verholpen d.m.v. verschillende beveiligingen tijdens het inloggen.

Inlogmethodes
VSBfonds kan via 2 scenario's inloggen:

1. Intern/op kantoor aan een docking station
2. Extern (thuis/op WI-FI)

Intern
Als er intern (aan een docking station) ingelogd wordt, is het invullen van een wachtwoord al voldoende om in een laptop te komen en om (zonder extra beveiliging) in de terminal server te komen. Na de overgang naar Dynamics is er geen terminal server waar de collega's op inloggen, maar kan je via de (op ingelogde) laptop, eenvoudig verschillende Cloud software in, waaronder SharePoint en Dynamics.

Extern
Zodra een collega extern aan het werken is (bijvoorbeeld vanaf huis), wordt er op dit moment naast een wachtwoord, ook een multi factor authenticatie (MFA) verstuurd naar een geregistreerde apparaat. Echter, wordt dit alleen gedaan als er verbinding wordt gemaakt met de terminal server. Zodra, wij over gaan naar Dynamics, zal een Microsoft MFA komen die toegang tot Dynamics beoordeeld. Momenteel wordt dit nog gedaan door DUO Mobile, waar VSBfonds per gebruiker voor betaald.

De handelingen die door VSBfonds gehanteerd worden, zijn volgens de (nieuwe) BDO authenticatie regels niet voldoende om een positieve notering te krijgen.
De BDO minimum practice stelt de volgende wachtwoordeisen (in het groen wat wij al doen):

- het initieel wijzigen van wachtwoorden wordt afgedwongen;
- het wachtwoord dient uit minimaal 6 karakters te bestaan;
- het wachtwoord dient complexe tekens te bevatten;
- het wachtwoord dient na maximaal 180 dagen te worden gewijzigd;
- de laatste 3 gebruikte wachtwoorden mogen niet worden hergebruikt;
- blokkade van gebruiker na 7 foutieve aanlogpogingen.

In 2020 heeft Tessa Askamp een wachtwoordbeleid document (in de bijlages toegevoegd) geschreven die een extra punt van de bovenstaande criteria zou raken. Hier werd aangegeven dat er een complexe wachtwoord gemaakt moest worden van minimaal 8 karakters en dat er om de 90 dagen een nieuwe wachtwoord aangemaakt moet worden. Zoals hiervoor geschreven, wordt dat laatste niet gedaan.

In het wachtwoorden beleid document van BDO (te vinden in de bijlage), staat ook dat de best practices van bedrijven zoals Microsoft goede richtlijnen/start punten zijn (niet volledig) om door de BDO jaarrekeningcontrole heen te komen.

Volgens Microsoft is alleen een wachtwoord aanpassen niet voldoende. Als wij om de 90 dagen een nieuwe wachtwoord moeten invullen en aan alle eisen moet voldoen, zal de kwaliteit van een wachtwoord omlaag gaan.

- Volgens de regels van BDO wachtwoord dag 1: Welkom01!
- Wachtwoord na 90 dagen: Welkom02!
- Wachtwoord volgende ronde: Welkom03!

Dit heeft te maken met het menselijke factor in authenticatie. We willen een wachtwoord aanmaken die we altijd kunnen herinneren. De wachtwoorden worden opgeschreven in boekjes of in browsers automatisch opgeslagen.

Microsoft raadt aan om een single sign-on (sso) in te stellen, zodat we voor alle Microsoft producten dezelfde inlogmethode hebben. Gelukkig, zullen wij met het gebruik van Dynamics, maar 1 inlog hebben. Alles gaat via een Microsoft account. Daarnaast, moet Microsoft Authenticator ingesteld worden om te controleren/bevestigen dat de persoon daadwerkelijk degene is die het ook aanvraagt. Hiervoor, werd al aangegeven dat dit huidig via DUO mobile gaat. Het idee, is dat de authenticatie vanaf 3 april 23 via Microsoft Authenticator gaat.

Microsoft Authenticator voordelen	Duo Mobile voordelen
Ondersteunt biometrische authenticatie, zoals gezichtsherkenning en vingerafdrukscans Biedt back-up- en herstelopties voor accountinformatie	Ondersteunt meerdere platforms (iOS, Android, Windows Phone) Ondersteunt een breed scala aan authenticatiemethoden, waaronder pushmeldingen, SMS-wachtwoorden, telefoon terugbellen en hardwaretokens.
Werkt met Microsoft-accounts en andere populaire diensten zoals Google en Facebook	Biedt de mogelijkheid om meerdere apparaten te registreren en te beheren
Komt in het Microsoft 365 business pakket. Geen extra kosten.	Biedt gedetailleerde rapportage en analyses voor beheerders

Microsoft Authenticator Nadelen	Duo Mobile Nadelen
Beperkte rapportage en analyse voor beheerders	Kosten: Betaald per gebruiker per maand.
Kan extra instelstappen vereisen voor sommige diensten	Beperkte integratie met Azure Active Directory

Beide DUO Mobile en Microsoft Authenticator zullen voor VSBfonds geschikt zijn. Doordat, Microsoft Authenticator geen extra kosten heeft, staat het er beter voor dan DUO Mobile.

Opties

Optie 1: Volgens BDO Minimal practice

BDO wilt dat de authenticatie minimaal geregeld wordt d.m.v. een complexe wachtwoord die maximaal 180 dagen geldig is. Daarnaast, mag een wachtwoord niet hetzelfde zijn, als de 3 vorige gebruikte wachtwoorden. Als je een wachtwoord meerdere keren verkeerd hebt ingevoerd, moet het account op inactief gezet worden, tot er een nieuw wachtwoord aangemaakt wordt door de gebruiker.

De eisen aan een wachtwoord moeten voldoen aan een bepaalde complexiteit. Zo dienen er minimaal 6 karakters in voor te komen en zal het speciale tekens moeten bevatten (zoals een !, ? of een @).

Daarbij, is het van belang om een multi factor authenticatie (MFA) toe te voegen bij het inloggen, om zo het gevaar van verloren/gekraakte wachtwoorden tegen te gaan.

Voordelen	Nadelen
Het gebruik van een complex wachtwoord met speciale tekens en een minimale lengte van 6 karakters verhoogt de beveiliging van het systeem.	Het verplicht wijzigen van wachtwoorden kan ertoe leiden dat medewerkers minder complexe wachtwoorden kiezen, waardoor de beveiliging mogelijk verzwakt wordt.
Het verplicht wijzigen van wachtwoorden na 180 dagen helpt voorkomen dat wachtwoorden te lang in gebruik blijven en dus vatbaar worden voor hacking.	Blokkade van gebruikers na 7 foutieve aanlogpogingen kan leiden tot beperkingen voor medewerkers die per ongeluk meerdere keren een verkeerd wachtwoord invoeren.
Het niet kunnen hergebruiken van de laatste 3 gebruikte wachtwoorden vermindert de kans op gehackte accounts.	Het verplicht wijzigen van wachtwoorden en het gebruik van complexe wachtwoorden kan het risico vergroten dat medewerkers wachtwoorden opschrijven of opslaan op een ander apparaat, wat de beveiliging kan verzwakken.
Blokkade van gebruikers na 7 foutieve aanlogpogingen vermindert de kans op brute-force attacks. (Ze kunnen anders onverhinderd door proberen)	Het verplicht wijzigen van wachtwoorden kan leiden tot extra administratieve taken voor de IT-afdeling en kan leiden tot extra kosten voor trainingen en support.
Multifactor authenticatie verhoogt de beveiliging doordat gebruikers zich niet alleen met een wachtwoord, maar ook met een tweede authenticatiemethode moeten identificeren.	

Optie 2: Volgens VSBfonds

Bij VSBfonds gebruiken wij een hybride variant van optie 1. Makkelijk te onthouden wachtwoord + MFA. Om ons eigen methode te versterken, zouden wij een complexe wachtwoord kunnen eisen volgens de BDO regels, maar niet een regelmatige aanpassing van het wachtwoord. In plaats daarvan zou er gebruik gemaakt worden van Microsoft Authenticator om één keer per dag of per (aanpassing van) netwerk identificatie te verifiëren dat de gebruiker is wie hij of zij beweert te zijn. Dit zou helpen bij het verminderen van het risico van gekraakte wachtwoorden en andere vormen van cyberaanvallen, terwijl het vermijden van de nadelen van regelmatige wachtwoordwijzigingen. Daarnaast, is het van belang om een blokkade te plaatsen op vaak verkeerde invoer bij een wachtwoord. Na 7x wordt er een blokkade op een account gezet, die alleen opgelost kan worden door de functioneel/it beheerder.

Het is echter belangrijk om te vermelden dat deze versie minder streng is dan optie 1. Hoewel deze optie nog steeds een versterking is ten opzichte van de huidige situatie, kan het zijn dat het niet voldoende is om aan de BDO authenticatie regels te voldoen. Het is daarom belangrijk om te begrijpen dat dit al besproken is met de IT-auditor Mark Schotsman om te achterhalen of het voldoende zou zijn. (Volgens Mark Schotsman wel!).

Een collega moet hierdoor, vaker (dan gewoonlijk) een authenticatie aanvraag goedkeuren. Dit zal ervoor zorgen dat er niemand ongeoorloofd op een systeem kan werken.

Voordelen	Nadelen
Te onthouden wachtwoord: doordat er geen regelmatige wachtwoordwijzigingen zijn en minder snel opschrijven of in een onveilige locatie opslaan.	Minder streng dan optie 1: doordat er geen regelmatige wachtwoordwijzigingen zijn
MFA: door het gebruik van Microsoft Authenticator wordt de veiligheid verhoogd doordat er een extra identificatiestap wordt toegevoegd aan het inlogproces. Dit vermindert het risico op inbreuken door middel van gekraakte wachtwoorden of andere vormen van cyberaanvallen.	Blokkade van gebruikers na 7 foutieve aanlogpogingen kan leiden tot beperkingen voor medewerkers die per ongeluk meerdere keren een verkeerd wachtwoord invoeren.
Versterking ten opzichte van de huidige situatie: door het implementeren van deze hybride variant is er een duidelijke versterking van de huidige beveiligingsmaatregelen voor een nieuw systeem.	Risico op zwakkere wachtwoorden: doordat er geen regelmatige wachtwoordwijzigingen zijn, bestaat er een risico dat gebruikers minder complexe wachtwoorden kiezen die makkelijker te raden zijn. Dit kan resulteren in een toename van het risico op inbreuken door middel van gekraakte wachtwoorden
Is al overlegd met Mark Schotsman en wordt gezien als een optie die voldoet aan de authenticatie regels.	

Aanbeveling:

Optie 2 wordt door mij aanbevolen, omdat dit het beste van beide werelden is. Hierdoor, kunnen collega’s hun wachtwoord goed onthouden, maar is het ook enorm secuur. Met deze aanpassingen kunnen wij eenvoudig aan de authenticatie eisen voldoen.

Door het implementeren van een optie 2 waarbij we een makkelijk te onthouden wachtwoord combineren met een dagelijkse MFA, kunnen we de risico's van gekraakte wachtwoorden en andere vormen van cyberaanvallen verminderen, terwijl we de nadelen van regelmatige wachtwoordwijzigingen vermijden.

Bijlages:

- Microsoft Authenticatie: Authentication with Azure AD - Microsoft Azure Well-Architected Framework | Microsoft Learn
- BDO Authenticatie: BDO - Authenticatie.pdf
- Wachtwoordbeleid 2020: Wachtwoordbeleid.docx