ARBONIA
IT SECURITY

Nieuw wachtwoordbeleid van de Arbonia-groep

Beste medewerkers,

Een sterk wachtwoord is de eerste verdedigingslinie voor onze systemen en gegevens.

Het hoofddoel van aanvallers is onder meer het stelen van toegangsgegevens van een gebruikersaccount om toegang te krijgen tot onze netwerken, servers en IT-systemen en in het ergste geval onopgemerkte activiteiten uit te voeren zoals gegevensdiefstal, spionage of het installeren van malware. Daarom vormen zwakke of gecompromitteerde wachtwoorden en het oneigenlijk gebruik ervan een aanzienlijk risico. Om beter te voldoen aan onze beveiligingseisen en om u beter te beschermen tegen deze bedreigingen, is er een nieuw wachtwoordbeleid gedefinieerd voor de Arbonia-groep.

Wijziging van het wachtwoordbeleid

Hieronder vindt u de volledige wachtwoordstrategie overzichtelijk weergegeven. De wijziging heeft vooral invloed op de minimale lengte van een wachtwoord, de maximale geldigheid van een wachtwoord en de complexiteit.

De minimale lengte van een wachtwoord is gewijzigd van momenteel 8 naar 12 tekens om het kraken van een wachtwoord te bemoeilijken, maar tegelijkertijd is het wachtwoord minimaal 360 dagen geldig. Als u een langer wachtwoord gebruikt (≥ 16 tekens), is het wachtwoord 540 dagen geldig. In alle gevallen moet bij de nieuwe wachtwoorden gezorgd worden voor een hoge mate van complexiteit (= sterk wachtwoord). Dit wordt bereikt door een combinatie van hoofdletters/kleine letters/cijfers 0–9/leestekens of speciale tekens.

Het gebruik van reeds gecompromitteerde wachtwoorden die vrij toegankelijk zijn op het internet en woorden van een zwarte lijst (bijvoorbeeld bedrijfsnamen) worden automatisch voorkomen.

Als het wachtwoord in een database met gecompromitteerde wachtwoorden zou verschijnen terwijl het nog geldig is, wordt u automatisch gevraagd om het wachtwoord te wijzigen.

Het nieuwe wachtwoordbeleid wordt automatisch geactiveerd de volgende keer dat u het Windows-wachtwoord wijzigt of op verzoek van uw lokale IT-afdeling. U ontvangt een herinnering 14 dagen voordat uw wachtwoord verloopt. **Het beleid geldt echter voor alle ICT-systemen van de Arbonia-groep, dus ook voor niet-Windows-systemen. Als houder van de account bent u in ieder geval verantwoordelijk voor de naleving van het wachtwoordbeleid, ook als dit technisch niet wordt afgedwongen.**

Een sterk wachtwoord aanmaken

Er zijn verschillende technieken om een sterk wachtwoord aan te maken en te onthouden. Maak bijvoorbeeld een sterk wachtwoord op basis van een zin of door gedefinieerde tekenreeksen te vervangen:

- Kies een zin die u gemakkelijk kunt onthouden en zet deze om in een wachtwoord. Bijv.: *"Het is helemaal niet moeilijk om een sterk wachtwoord te kiezen."* Gebruik de eerste paar letters of meerdere letters van de afzonderlijke woorden en verrijk het wachtwoord met cijfers en speciale tekens. Bijv.: *"Hihnmo1swtk."*
- Kies een woord dat u gemakkelijk kunt onthouden, bijvoorbeeld "Namiddag" en definieer een speciale tekenreeks, bijvoorbeeld *"1$1"*. Vervang nu gedefinieerde delen/letters van het woord door de door u gekozen tekenreeks om een sterk wachtwoord te krijgen. Bijv.: *"N1$1midd1$1g"*

Dank u voor uw medewerking en vriendelijke groeten,
Arbonia Security Team

ARBONIA
IT SECURITY

Wachtwoordstrategie			
Wachtwoordgeschiedenis (aantal vorige wachtwoorden dat niet opnieuw kan worden gebruikt)	5	**Aantal mislukte inlogpogingen voor het account wordt vergrendeld**	6
Minimale lengte van het wachtwoord	12 tekens	**Duur van de vergrendeling van de account**	Totdat een beheerder ontgrendelt
Maximale geldigheid van een wachtwoord	360 dagen (12–15 tekens) of 540 dagen (≥16 tekens)	**Duur tot de teller van mislukte inlogpogingen wordt gereset**	≥ 60 minuten
Complexiteit	➢ Hoofdletters ➢ Kleine letters ➢ Cijfers 0–9 ➢ Leestekens of speciale tekens	**Specifiek (Windows-wachtwoorden – intern voor Arbonia en wordt automatisch afgedwongen)**	Het wachtwoord mag geen cijfers op de eerste of laatste positie of 3 opeenvolgende identieke tekens bevatten

Gebruik geen wachtwoorden die in dit document als voorbeeld worden gegeven. Deze voorbeeldwachtwoorden zijn nu 'gecompromitteerd' en staan op de zwarte lijst.

Let naast deze informatieve brief ook op het geldige wachtwoordbeleid (IS-ISP-GROUP-001-PASSWORD-POLICY) op https://security.arbonia.com

Wanneer u uw Windows-wachtwoord wijzigt, krijgt u de vereisten te zien waaraan moet worden voldaan.