POLITIE

Interne Memo

Onderwerp
Herzien wachtwoordbeleid
Politie Intern en Confidentieel

Organisatieonderdeel
PDC
Dienst ICT

Behandeld door
5.1.2.e

Functie

Telefoon
+31 6 5.1.2.e

E-mail
5.1.2.e @politie.nl

Ons kenmerk

Uw kenmerk

In afschrift aan

Datum
14 januari 2020

Bijlage(n)
0

Pagina
1

LS,

Inleiding:
De huidige methodiek van gebruikersnaam / wachtwoord is niet meer veilig genoeg, we moeten naar een beter, veiliger toegangssysteem van onze ICT toe.
Met de toenemende frequentie en impact van cyberaanvallen en huidige rekenkracht van computers is het achterhalen van het wachtwoord van een gebruiker steeds eenvoudiger. De wachtwoorden bij politie zijn nu 5.1.2.i maar zouden eigenlijk nu al naar 5.1.2.i (conform nieuwe BIR) moeten en het wachtwoordbeleid zou aangepast moeten worden. Tevens heeft het oude principe van gebruikersnaam / wachtwoord heeft zijn langste tijd gehad; we moeten naar andere, betere authenticatie toe. De beste manier hiervoor is het toevoegen van een 5.1.2.i . Alternatief zou kunnen zijn 5.1.2.i Bijvoorbeeld voor Telewerken wordt 5.1.2.i nu gedaan met een 5.1.2.i .

Het huidige wachtwoordbeleid is vastgelegd in de uitvoeringsregelingen van de dienst ICT. Hiervan zijn in momenteel twee versies goedgekeurd, te weten de "uitvoeringsregeling politie intern" en de "uitvoeringsregeling politie confidentieel" en een derde uitvoeringsregeling voor het rubriceringsniveau politie geheim zit momenteel in de review fase.

Probleem:
Door de toename van het aantal Cyberaanvallen (CSBN2017 van het NCSC en rapport 'Een nooit gelopen race" van het Rathenau instituut) op bedrijven en overheden[1] en de steeds slimmere manier waarop hackers malware weten binnen te krijgen (of inlog-informatie afhandig weten te maken).

Deze onderzoeken hebben geleid tot een herziening van onder andere de kaders die de rijksoverheid gebruikt (BIR) en "de facto" standaarden zoals bijv. zijn vastgelegd in de NIST-800-63B

9.4.3	1	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
9.4.3.1	1	Als er geen gebruik wordt gemaakt van 5.1.2.i is de wachtwoordlengte 5.1.2.i en 5.1.2.i van samenstelling. Vanaf een wachtwoordlengte van 5.1.2.i vervalt de complexiteitseis. Het aantal inlogpogingen 5.1.2.i . De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
9.4.3.2	2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal

Figuur 1. Nieuwe standaarden BIR

1 https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html en ook https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race

Onderwerp
Herzien wachtwoordbeleid
Politie Intern en Confidentieel

Datum
14 januari 2020

Aanpassing wachtwoordbeleid uitvoeringsregelingen politie:
Alle uitvoeringsregelingen hebben een geldigheidstermijn van 2 jaar voordat deze worden geactualiseerd. Vooruitlopend op de herziening van deze uitvoeringsregelingen is het noodzakelijk om het wachtwoordbeleid van de politie aan te passen aan de hedendaagse werkelijkheid.

Het onderstaande herziene beleid is gebaseerd op de huidige uitvoeringsregeling politie confidentieel met een aantal aanscherpingen om aan te sluiten bij de kaders van de van de rijksoverheid. Het belangrijkste verschil tussen het nieuwe beleid en de huidige kaders is weergegeven in de onderstaande tabel.

Nieuw wachtwoordbeleid	**Huidig beleid**	
Politie intern en politie confidentieel	*Politie intern*	*Politie confidentieel*
5.1.2.i of 5.1.2.i	5.1.2.i	5.1.2.i of 5.1.2.i

Hierbij wordt opgemerkt dat het gebruiken van 5.1.2.i voor een wachtwoord naar verwachting door de medewerkers niet als gebruiksvriendelijk zal worden ervaren. Het is dus verstandig om waar mogelijk gebruik te maken van 5.1.2.i in combinatie met '5.1.2.i", om hiermee de gebruiksvriendelijkheid te vergroten.

Het verlopen van de wachtwoorden is voor als nog gebleven 5.1.2.i om te voorkomen dat de diverse wachtwoorden onderling een andere termijn hebben waarin ze verlopen. Vanuit beveiligingsperspectief 5.1.2.i

Met de ondertekening van dit memo vervallen de overlappende kaders uit de uitvoeringsregeling Politie intern en confidentieel en wordt het onderstaande wachtwoordbeleid van toepassing. Bij het herzien van de betreffende uitvoeringsregelingen zal het aangepaste wachtwoordbeleid worden verwerkt.

Voor akkoord:

Naam:	5.1.2.e
Hantekening:	5.1.2.e
Datum:	15-1-2020

Onderwerp
Herzien wachtwoordbeleid
Politie Intern en Confidentieel

Datum
14 januari 2020

Wachtwoordbeleid Politie Intern

Gebruik van wachtwoorden

Het gebruik van wachtwoorden wordt opgedeeld in drie categorieën namelijk gebruikerswachtwoorden, privileged (admin of beheer) accounts en service account wachtwoorden.

Gebruikerswachtwoorden

Medewerkers (gebruikers) behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van
wachtwoorden. Eind 2014 is in het kader van IAM onderstaande regeling hiervoor in gebruik genomen:

Uitvoeringsregeling "Identificatie en authenticatie van gebruikers middels wachtwoorden".

Algemeen.
Bij het aanmelden aan informatiesystemen identificeert de gebruiker zich middels zijn of haar accountnaam. De identiteit van de gebruiker wordt vervolgens vastgesteld (authenticatie) door het invoeren van een wachtwoord en/of door het gebruik van hard-, of soft- tokens en/of Biometrie.
Deze uitvoeringregeling beschrijft de beveiligingseisen waaraan het account ten aanzien van het identificatieproces moet voldoen, alsmede de eisen die aan het wachtwoord en het gebruik van het wachtwoord worden gesteld. Wachtwoordlengtes van 5.1.2.i *worden toegestaan evenals het gebruik van alle mogelijke karakters en leestekens..*
Het gebruik van de andere middelen voor authenticatie worden in deze uitvoeringsregeling buiten beschouwing gelaten.

Beveiligingseisen ten aanzien van het account met betrekking tot de identificatie van de gebruiker:

1) *Iedere gebruiker identificeert zich middels zijn accountnaam;*
2) *Iedere handeling vanuit een account is tot een natuurlijk persoon herleidbaar;*
3) *Iedere accountnaam is uniek;*
4) *Iedere gebruiker heeft 1 uniek account. Indien in de praktijk dit uitgangspunt nog niet gerealiseerd kan worden dient ten minste een zodanige inrichting plaats te vinden dat het voor een ieder helder is: "dat het één en dezelfde gebruiker betreft."*
5) *Iedere beheerder heeft aanvullend op het voorgaande punt 1 uniek account voor beheeractiviteiten;*
6) *De accountnaam is betekenisloos en bevat dus geen gegevens over de functie, afdeling of soort werkzaamheden van de gebruiker;*
7) *Het gebruikersaccount van de eerder aangemelde gebruikers mag tijdens het inloggen van de volgende gebruiker niet getoond worden.*
8) *Authenticatie van de gebruiker vindt plaats via* 5.1.2.i .

Beveiligingseisen ten aanzien van het wachtwoord en het gebruik van het wachtwoord.

1) *Een wachtwoord dient te voldoen aan de volgende eisen:*
   1) *Moet voor gebruikers* 5.1.2.i *lang zijn en voor beheeraccounts* 5.1.2.i *. In beide gevallen is een* 5.1.2.i *aanvullend noodzakelijk. Indien* 5.1.2.i *voor de gebruikersaccounts niet mogelijk is wordt een wachtwoord vereist van* 5.1.2.i
   2) *Mag niet de inlognaam (accountnaam), roepnaam en/of achternaam bevatten*

3) *Wachtwoorden die op een blacklist staan mogen niet worden gebruikt.*
4) *Bevat karakters* 5.1.2.i *:*
   a. *hoofdletters (A t/m Z)*
   b. *kleine letters (a t/m z)*
   c. *cijfers (0 t/m 9)*
   d. *leestekens (bijvoorbeeld:-, !, $, #, %)*
   Deze complexiteitseisen zijn niet vereist indien 5.1.2.i *wordt toegepast of indien* 5.1.2.i *worden gebruikt.*

2) *Na het* 5.1.2.i *van een foutief wachtwoord, wordt de toegang geblokkeerd en dient reset via Servicedesk of tool (voor primair wachtwoord) plaats te vinden;*
3) *Na het* 5.1.2.i *foutief toepassen van de wachtwoord resettool wordt de het account geblokkeerd en kan reset slechts plaatsvinden via de Servicedesk na adequate authenticatie (waartoe nog nadere regels worden vastgesteld);*
4) *Gebruikers kunnen op elk moment hun wachtwoord wijzigen. Bij het wijzigen van het wachtwoord moet eerst dit oude wachtwoord worden ingegeven.*
5) *De gebruiker wordt* 5.1.2.i *gedwongen zijn wachtwoord te wijzigen. De gebruiker wordt* 5.1.2.i *hiervan in kennis gesteld.*
6) *Indien de gebruiker niet beschikt over het oude wachtwoord, dient voorafgaande aan een reset van het wachtwoord, via andere middelen de authenticiteit van de aanvrager voldoende gewaarborgd te worden.*
7) *Hergebruik van eerder gebruikte wachtwoorden is* 5.1.2.i
8) *Gebruikers kunnen hun wachtwoord* 5.1.2.i *wijzigen.*
9) *Een tijdelijk wachtwoord (zoals bijvoorbeeld uitgegeven door beheer, Servicedesk of via SMS) wordt tijdens de eerstvolgende inlogsessie van de gebruiker door de laatste gewijzigd.*
10) *Een tijdelijk wachtwoord is* 5.1.2.i *geldig*
11) *Niet tijdelijke wachtwoorden worden alleen versleuteld verzonden.*
12) *Wachtwoorden worden alleen versleuteld en niet-decodeerbaar opgeslagen*

Afwijken van deze beveiligingseisen kan alleen nadat via het Team Informatiebeveiliging (Dienst IM), dan wel de afdeling Veiligheid en Continuïteit (Dienst-ICT) een risicoanalyse heeft plaatsgevonden en goedkeuring is verleend door de CISO. Iedere afwijking wordt gedocumenteerd.

Privileged (admin of beheer) accounts wachtwoorden
Bij het aanmaken van privileged (admin) account wachtwoorden behoort men goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

Aan privileged (admin) account wachtwoorden is een set gedragsregels aangereikt met daarin minimaal het volgende:

1. *Wachtwoorden worden niet opgeschreven (of op een andere wijze onbeveiligd opgeslagen);;*

1) *Elk privileged (admin) account heeft een uniek wachtwoord;*
2) *Het wachtwoord moet* 5.1.2.i *worden gewijzigd;*
3) *Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde;*
4) *het account wordt aangemaakt conform de naamgevingconventie zodat de functie en gerelateerde dienst/applicatie herleidbaar is;*
5) *het wachtwoord is* 5.1.2.i *, alfanumeriek met vreemde tekens;*
6) *Wachtwoord mag niet gelijk zijn aan* 5.1.2.i *.*
7) *Beheerders kunnen hun wachtwoord* 5.1.2.i *zelf wijzigen.*

Postbus 238
3970 AE Driebergen
Zeisterweg 1b
3984 NH Odijk
www.politie.nl

8) *het account is herleidbaar naar een natuurlijk persoon; er wordt een eigenaar gekoppeld;*
9) *het account zelf wordt zodanig ingeregeld dat mogelijk misbruik wordt geminimaliseerd.*
10) *Lock-out* 5.1.2.i
11) *Authenticatie van een privileged account vindt plaats* 5.1.2.i

Service account wachtwoorden

Bij het aanmaken van wachtwoorden voor service accounts behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

Aan service account met hoge rechten is een set gedragsregels aangereikt met daarin minimaal het volgende:

1. *Wachtwoorden worden niet opgeschreven(of op een andere wijze onbeveiligd opgeslagen);*
2. *Elk service account heeft een uniek wachtwoord;*
3. *Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde;*
4. *het account wordt aangemaakt conform de naamgevingconventie zodat de functie en gerelateerde dienst/applicatie herleidbaar is;*
5. *het wachtwoord wordt via een procedure door het systeem* 5.1.2.i
6. *het wachtwoord is* 5.1.2.i *, alfanumeriek met vreemde tekens*[3]*;*
7. *het account is herleidbaar naar een natuurlijk persoon; er wordt een eigenaar gekoppeld;*
8. *het account zelf wordt zodanig ingeregeld dat mogelijk misbruik wordt geminimaliseerd.*

Maatregelen op het Service account zelf:

1. *Policy User Rights Assignment:*
   5.1.2.i
   5.1.2.i

Functionele accounts

Functionele accounts dienen zoveel mogelijk te worden vermeden maar kennen dezelfde wachtwoordeisen als een gewoon gebruikersaccount. Ook de rechten van een dergelijk account is zo veel mogelijk beperkt tot het noodzakelijke.

---

[2] Voor Linux systemen 5.1.2.i
[3] De beleidsregel schrijft 5.1.2.i voor, na risicoanalyse en op verzoek van IVC is dit aangescherpt