PREVENTIEKAART

WACHTWOORDEN

Zomer 2023

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Inloggegevens blijven heel gewild bij hackers. Door diefstal c.q. datalekken circuleren miljoenen wachtwoorden online. Daarom zijn duidelijke afspraken over wachtwoorden gewenst. Dit beleid geldt voor iedereen in elke organisatie. Hierbij helpen onderstaande adviezen, die het meest effectief zijn in combinatie met multifactor authenticatie.

1 > SNAP HET WACHTWOORDBELEID

Zorg dat iedereen in de organisatie weet waarom de moeite nodig is en hoe snel een wachtwoord te kraken valt. Zeker met de komst van kunstmatige intelligentie.

2 > MAAK VOOR ELK GEBRUIKERSACCOUNT EEN ANDER WACHTWOORD

Door steeds een uniek wachtwoord te gebruiken, kan de schade beperkt blijven als een wachtwoord gestolen wordt. Wie diefstal vermoedt, hoeft dan maar één nieuw wachtwoord te maken.

3 > GEBRUIK MINIMAAL 13 KARAKTERS, MAAR LIEVER 18 OF NOG LANGER

Een lang wachtwoord is sterk omdat deze moeilijker te kraken is dan een kort wachtwoord, waarvoor algoritmes bestaan. Vanwege die algoritmes moet je nooit een wachtwoord maken met enkel nummers of letters; die zijn namelijk razendsnel te ontcijferen. De wachtwoorden van reguliere gebruikers moeten minstens 13 karakters lang zijn, die van een beheerder (Admin) minstens 18, al heeft een nog langere wachtwoordzin de voorkeur.

4 > ZORG DAT WACHTWOORDEN ONVOORSPELBAAR ZIJN

Kwaadaardige hackers houden ellenlange lijsten bij met voorspelbare en bekende wachtwoorden, zoals Welkom1234! en Pa55word!. Deze zijn voor hackers vrij eenvoudig te raden. Vermijd daarom in ieder geval beginnen met een hoofdletter en eindigen met twee cijfers of een uitroepteken.

Onvoorspelbaar is:

a. Een willekeurige combinatie van hoofdletters, kleine letters, cijfers en speciale karakters (inclusief een spatie), bijvoorbeeld: d%6Wo x27!PMn@ _L#&qe
b. Een onlogische wachtwoordzin met diverse karakters, bijvoorbeeld: P@niek loopt IN 189 wolken
c. Het gebruik van drie willekeurige woorden met een minimale lengte van 18 karakters, bijvoorbeeld: KlapRoos-AutoRit ZonneBrand

5 > VERMIJD HERGEBRUIK

Zorg dat medewerkers zo min mogelijk inloggegevens met elkaar delen. Pas dan is er sprake van unieke en daarmee meest veilige informatie.

6 > OVERWEEG HET GEBRUIK VAN EEN PASSWORD MANAGER

Het is ondoenlijk om alle unieke, sterke wachtwoorden te onthouden. Daarom zijn er veel producten voor wachtwoordbeheer op de markt. Deze wachtwoordmanagers zijn misschien niet perfect, maar bieden voldoende voordelen om veilig te kunnen werken. Zo kunnen veel wachtwoordmanagers unieke, lange en willekeurige wachtwoorden maken voor alle accounts. Online bestaan websites die password managers vergelijken, zoals techradar.com.

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant
Ministerie van Economische Zaken en Klimaat