Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Gebruik tweefactorauthenticatie

Wachtwoorden alleen zijn niet voldoende

Factsheet FS-2015-02 | versie 1.2 | 17 maart 2023

Accounts worden doorgaans beveiligd door middel van een gebruikersnaam en wachtwoord. Deze techniek is al tientallen jaren in gebruik en is de meest voorkomende manier om toegang te krijgen tot een account. Vaak kiest een gebruiker voor simpele wachtwoorden, omdat deze gemakkelijk te onthouden zijn. Dit maakt het eenvoudiger voor kwaadwillenden om toegang te krijgen tot accounts. Wanneer een kwaadwillende toegang krijgt tot een account, kan deze zich voordoen als de eigenaar van het account en het account misbruiken. Het NCSC adviseert gebruikers om overal waar dat kan gebruik te maken van tweefactorauthenticatie. Ook adviseert het NCSC om sterke wachtwoorden te hanteren en om een wachtwoordmanager te gebruiken. Met deze technieken kan een kwaadwillende moeilijker toegang krijgen tot accounts.

Achtergrond

Een gebruiker verkrijgt vaak toegang tot een account door een gebruikersnaam en wachtwoord in te voeren. De gemiddelde gebruiker beschikt tegenwoordig over tientallen persoonlijke en zakelijke accounts. Voorbeelden hiervan zijn accounts voor e-mail, sociale media, internetbankieren en online webwinkels. Het goed beveiligen van deze grote hoeveelheid accounts is noodzakelijk.

Doelgroep

Deze factsheet is hoofdzakelijk bedoeld voor thuisgebruikers.

Voor organisaties en bedrijven heeft het NCSC de factsheet "Volwassen authenticeren".[1] Daarnaast vind je op de website van het Digital Trust Center (DTC) extra informatie over het gebruik van tweefactorauthenticatie.[2]

Samenwerkingspartners

Logius, Rabobank, SIDN, Microsoft en het Digital Trust Center (DTC).

De belangrijkste adviezen

1. Het NCSC adviseert om overal waar dit kan gebruik te maken van tweefactorauthenticatie.
2. Omdat niet alle websites en diensten tweefactorauththenticatie aanbieden, adviseert het NCSC om ook een wachtwoordmanager te gebruiken voor het beheren en creëren van wachtwoorden.
3. Het NCSC adviseert om sterke wachtwoorden te gebruiken en het gebruiken van hetzelde wachtwoord voor verschillende accounts te voorkomen.

1 https://www.ncsc.nl/documenten/factsheets/2022/april/24/factsheet-volwassen-authentiseren-gebruik-veilige-middelen-voor-authenticatie

2 https://www.digitaltrustcenter.nl/tweefactorauthenticatie

Wat is tweefactorauthenticatie?

Wachtwoorden zijn al tientallen jaren in gebruik en zijn nog steeds de meest gebruikte vorm van authenticatie. Door te authenticeren verifieert het systeem of de gebruiker de daadwerkelijke eigenaar van het account is en autoriseert het systeem de gebruiker. Bij veel systemen wordt gebruik gemaakt van een tweede stap in de authenticatie, bijvoorbeeld door controle van een extra code die een gebruiker moet invoeren. De laatste jaren worden ook andere technieken steeds meer ingezet als authenticatiemiddel. Een voorbeeld hiervan is het gebruik van een gezichtsscan of een vingerafdruk.

Een gebruiker kan zich op drie verschillende manieren authenticeren. Deze manieren worden ook wel factoren genoemd:

- iets wat je weet (bijvoorbeeld een wachtwoord of een pincode);
- iets wat je hebt (bijvoorbeeld een telefoon of een zogenaamde token);
- iets wat je bent (bijvoorbeeld een gezichtsscan of een vingerafdruk).

Als een gebruiker minimaal twee van deze factororen combineert is er sprake van tweefactorauthenticatie

Wat is er aan de hand?

Veel gebruikers loggen in op basis van slechts één van de bovenstaande factoren, doorgaans een wachtwoord of pincode (iets dat je weet). Daarnaast beschikt de gemiddelde gebruiker over meerdere accounts waarvoor een wachtwoord nodig is om in te loggen. In de praktijk betekent dit dat gebruikers vaak kiezen voor simpele wachtwoorden. Dit wachtwoord, of een simpel te raden variant ervan, wordt vaak voor meerdere accounts gebruikt. Verder worden wachtwoorden niet veilig bewaard maar bijvoorbeeld opgeschreven op papier of onversleuteld opgeslagen op de computer of mobiele telefoon.

Wat kan er gebeuren?

Bij gebruik van simpele wachtwoorden kan een kwaadwillende makkelijker toegang krijgen tot accounts. Met behulp van lijsten van veelgebruikte wachtwoorden kan een aanvaller proberen toegang te krijgen tot een account. Ook er kunnen er technieken ingezet worden om een wachtwoord te achterhalen door combinaties van letters, cijfers en symbolen te proberen (brute force). Hoe korter het wachtwoord, hoe sneller een wachtwoord met het gebruik van rekenkracht kan worden gekraakt.

Wanneer een kwaadwillende toegang krijgt tot een account, kan deze zich voordoen als eigenaar van het account en hier misbruik van maken. Ook heeft de kwaadwillende dan persoonlijke informatie van de gebruiker tot zijn beschikking. Deze informatie kan bestaan uit adresgegevens, een geboortedatum, een bankrekeningnummer of een telefoonnummer, maar ook uit bijvoorbeeld medische of financiële gegevens. Bovendien kan een kwaadwillende bekijken of de gebruiker het wachtwoord ook gebruikt voor andere accounts. Wanneer dit het geval is, kan de kwaadwillende nog meer persoonlijke informatie van de gebruiker achterhalen. Deze gegevens kunnen vervolgens gebruikt worden om bijvoorbeeld fraude te plegen.

Naast gerichte aanvallen op een specifiek account, kan ook een wachtwoordendatabase van een website of systeem het doelwit zijn. De kans op een succesvolle aanval hangt in dit geval af van de beveiliging van het systeem of de website zelf. De afgelopen jaren vonden meerdere grootschalige datalekken plaats waarbij informatie over accounts op het internet werd gepubliceerd. Dergelijke aanvallen vallen buiten de controle van een gebruiker. Wanneer een gebruiker hetzelfde wachtwoord voor meerdere accounts gebruikt, wordt het risico groter dat een kwaadwillende

door een groot datalek toegang krijgt tot meer dan één account.[3]

Wat kunt u doen?

Zoals hiervoor wordt het beschreven is enkel een wachtwoord niet meer voldoende. Gelukkig zijn er veilige alternatieven. Het NCSC adviseert om, waar dat kan, tweefactorauthenticatie te gebruiken. Mocht het niet mogelijk zijn om tweefactorauthenticatie in te schakelen, dan adviseert het NCSC om gebruik te maken van een wachtwoordmanager om sterke wachtwoorden te beheren en te creëren.

1. Gebruik tweefactorauthenticatie

Het NCSC adviseert om, waar dat kan, gebruik te maken van tweefactorauthenticatie. Een andere naam hiervoor is tweestapsverificatie. Dit bestaat uit authenticatie door middel van twee van de drie factoren (iets wat je weet, iets wat je hebt en iets wat je bent).[4] Een voorbeeld hiervan is het gebruik van een wachtwoord en een vingerafdruk. Een andere mogelijkheid is de combinatie van een wachtwoord en een eenmalig te gebruiken authenticatiecode die bijvoorbeeld gegenereerd wordt in een tweefactorauthenticatie app (2FA app) op een smartphone.[5] In een enkel geval wordt een derde factor toegevoegd voor extra veiligheid.

Tweefactorauthenticatie is veiliger dan het gebruik van alleen een wachtwoord, omdat toegang tot een account niet verkregen kan worden door enkel het wachtwoord te achterhalen. Om toegang te kunnen krijgen moet een kwaadwillende tegelijkertijd ook in het bezit zijn van biometrische data van de gebruiker of een fysiek element zoals een token of telefoon. Dit verkleint de kans dat een kwaadwillende erin slaagt om toegang te krijgen tot accounts. Een groeiend aantal diensten biedt tegenwoordig tweefactorauthenticatie aan of verplicht het gebruik hiervan.[6] Sommige internetdiensten bieden de mogelijkheid om via een andere identiteitsdienst in te loggen, bijvoorbeeld met behulp van een Google- of Facebook-account. Een voordeel van inloggen via dergelijke diensten is dat met deze methode tweefactorauthenticatie wordt afgedwongen indien de gebruiker dit heeft geactiveerd voor de betreffende dienst. De gebruiker moet dit vaak wel zelf aanzetten en het advies is dan ook om dit overal te doen.

2. Gebruik een wachtwoordmanager

Helaas bieden nog niet alle websites en diensten tweefactorauthenitcatie aan. Daarom adviseert het NCSC om ook een wachtwoordmanager te gebruiken. Dit is een hulpmiddel om wachtwoorden digitaal te beheren. Met een wachtwoordmanager is het mogelijk om wachtwoorden versleuteld op te slaan. Om toegang te krijgen tot de wachtwoordmanager hoeft de gebruiker slechts één sterk hoofdwachtwoord te onthouden. Dit is een groot voordeel van een wachtwoordmanager. Alle wachtwoorden voor andere diensten worden opgeslagen in de

[3] Deze website checkt of jouw emailadres (en bijbehorend account) voorkomt in een data lek. De kans is dan zeer groot dat jouw wachtwoord ook gelekt is: https://haveibeenpwned.com/

[4] Zie pagina 3 van deze factsheet voor een uitgebreidere bespreking van deze factoren

[5] Voor meer hulp bij kiezen van een goede 2FA app, kijk op deze website: https://www.nytimes.com/wirecutter/reviews/best-two-factor-authentication-app/ of deze website https://www.pcmag.com/picks/the-best-authenticator-apps

[6] Check op deze website of een website tweefactorauthenticatie aanbiedt: https://2fa.directory/nl/

wachtwoordmanager waardoor de gebruiker deze niet meer hoeft te onthouden. Deze wachtwoorden kunnen op elk moment worden opgevraagd bij de wachtwoordmanager. Hierdoor kan de gebruiker zeer complexe wachtwoorden gebruiken en kan er voor elk account een ander wachtwoord ingesteld worden. Het risico van een wachtwoordmanager is dat alle wachtwoorden op dezelfde plek worden bewaard. Wanneer de wachtwoordmanager wordt gecompromitteerd, kan de kwaadwillende toegang krijgen tot alle wachtwoorden van de gebruiker.[7] Het is daarom belangrijk dat de gebruiker een sterk en uniek hoofdwachtwoord kiest.

Er zijn twee typen wachtwoordmanagers: online en offline wachtwoordmanagers. Een online wachtwoordmanager is doorgaans gebruiksvriendelijker; een offline wachtwoordmanager biedt meer mogelijkheden om het beveiligingsniveau naar eigen inzicht en het vereiste niveau in te stellen (waarbij het beveiligingsniveau van het systeem waarop de wachtwoordmanager geïnstalleerd is een grote rol speelt).

Een online wachtwoordmanager

Dit type wachtwoordmanager maakt gebruik van clouddiensten om wachtwoorden op te slaan. Dit betekent dat wachtwoorden worden opgeslagen op een manier waarbij ze vanaf elke computer, tablet of mobiele telefoon met internetverbinding toegankelijk zijn. Wanneer de gebruiker in de wachtwoordmanager een wachtwoord wijzigt of een nieuw wachtwoord aanmaakt voor een nieuw account, synchroniseert de wachtwoordmanager het nieuwe wachtwoord naar alle apparaten wanneer deze verbinden met het internet. Het wachtwoord wijzigen is daardoor maar op één apparaat nodig. Voorbeelden van veel gebruikte online wachtwoordmanagers zijn 1Password en Dashlane.[8]

Een offline wachtwoordmanager

Dit type wachtwoordmanager bewaart wachtwoorden lokaal op een apparaat. De gebruiker moet om deze reden de wachtwoordmanager op meerdere apparaten installeren. Ook is het mogelijk om de software te installeren op een USB-stick. Met een USB-stick kan een gebruiker toegang krijgen tot zijn wachtwoorden op een computer waar deze niet zijn opgeslagen. De gebruiker zal wachtwoorden op elk apparaat of USB-stick handmatig moeten aanpassen, omdat de wachtwoordmanagers niet automatisch synchroniseren. Een voorbeeld van een offline wachtwoordmanager is Keepass.

Met een offline wachtwoordmanager is het ook mogelijk om het versleutelde bestand met wachtwoorden op te slaan bij een clouddienst. Op deze manier wordt het bestand gesynchroniseerd op alle apparaten waar de wachtwoordmanager is geïnstalleerd en de wachtwoorden zijn opgeslagen. De wachtwoordmanager is zo echter niet geheel offline.

Zowel online als offline wachtwoordmanagers kennen voor- en nadelen. Een voordeel van een online wachtwoordmanager is dat het beheer van wachtwoorden relatief eenvoudig is, omdat het synchroniseren automatisch gebeurt. Een nadeel van een online wachtwoordmanager is dat wachtwoorden in de cloud worden opgeslagen en de gebruiker de versleutelingstechniek van de wachtwoordmanager zal moeten vertrouwen. De gebruiker heeft namelijk geen controle over hoe er met de versleutelde wachtwoorden

[7] Special voor ondernemers geeftt het DTC ook advies over het gerbuik van wachtwoordmanagers: https://www.digitaltrustcenter.nl/hoe-kies-ik-een-wachtwoordmanager

[8] Er zijn meerdere websites die advies geven over wachtwoordmanageners. Wired is een voorbeeld hiervan: https://www.wired.com/story/best-password-managers/

wordt omgegaan in de cloud. Wanneer een kwaadwillende een kwetsbaarheid vindt in deze dienst, is het mogelijk dat de wachtwoorden van alle gebruikers op straat komen te liggen.

Een voordeel van een offline wachtwoordmanager is dat de gebruiker zelf de controle heeft over het beheer van zijn wachtwoorden. Wachtwoorden worden lokaal opgeslagen en de gebruiker is niet afhankelijk van de beveiliging van een clouddienst. De verantwoordelijkheid voor de beveiliging van de plek waar de wachtwoorden zijn opgeslagen ligt bij de gebruiker zelf. Een nadeel van een offline wachtwoordmanager is dat de gebruiker ook in dit geval de versleutelingstechniek van de wachtwoordmanager moet vertrouwen. Bovendien zal de gebruiker wachtwoorden handmatig moeten synchroniseren en dit vergt extra werk.

Bij zowel online als ook offline wachtwoordmanagers zal de gebruiker het hoofdwachtwoord van de wachtwoordmanager moeten onthouden. Wanneer deze wordt vergeten, heeft de gebruiker op dat moment geen toegang meer tot al zijn accounts en zal hij deze moeten laten resetten. Om dit te voorkomen, kan de gebruiker ervoor kiezen om het hoofdwachtwoord op papier te schrijven en dit op een veilige plek te bewaren, bijvoorbeeld in een kluis.

3. Kies sterke wachtwoorden

Het NCSC adviseert om sterke wachtwoorden te gebruiken. Een wachtwoord is sterk als:

- het lang is;
- het complex is. Dit houdt in dat een wachtwoord bestaat uit kleine letters, hoofdletters, spaties, cijfers en/of leestekens.

Sterke wachtwoorden zijn noodzakelijk omdat kwaadwillenden korte en simpele wachtwoorden snel kunnen kraken. Het NCSC is van mening dat wanneer de gebruiker een keuze moet maken tussen soorten wachtwoorden het beter is om lange wachtwoorden te kiezen dan complexe wachtwoorden. Er is een module gemaakt die test hoelang het duurt om een wachtwoord te kraken en geeft daarmee een indicatie over de sterkte van een wachtwoord.[9] Het is niet aan te raden om de sterkte van wachtwoorden te laten bepalen door diensten die vragen om het betreffende wachtwoord in te vullen. Het is vaak niet duidelijk wat deze diensten met ingevoerde wachtwoorden doen.

Voor het hoofdwachtwoord van de wachtwoordmanager kan de gebruiker bijvoorbeeld kiezen voor een wachtzin met een lengte van dertig tekens. Een wachtzin bestaat uit een aantal woorden die achter elkaar geplakt zijn. Door een aantal woorden op een willekeurige manier achter elkaar te zetten, kan de gebruiker een lang wachtwoord vormen. Ook kan hij hier cijfers, leestekens of spaties aan toevoegen. Het NCSC adviseert om woorden te kiezen die geen direct verband met elkaar hebben om zo de kans dat een kwaadwillende een wachtwoord raadt te verkleinen. Het is bijvoorbeeld niet verstandig om een zin afkomstig uit een boek of songtekst als wachtwoordzin te kiezen.

De wachtwoorden die de gebruiker opslaat in de wachtwoordmanager kan deze laten genereren door de wachtwoordmanager. Hiermee wordt meteen sterk wachtwoord gekozen

Het NCSC adviseert om wachtwoorden slechts voor één account te gebruiken. Door het hergebruiken van wachtwoorden kan een kwaadwillende die toegang heeft verkregen tot één account veel makkelijker toegang krijgen

[9] http://www.jewachtwoord.nl/

tot andere accounts die hetzelfde wachtwoord gebruiken. Dit is ook het geval wanneer wachtwoorden kleine variaties zijn van andere wachtwoorden.

In enkele gevallen is het noodzakelijk om wachtwoorden te vervangen. Dit is het geval wanneer een datalek bij een internetdienst heeft plaatsgevonden en de gebruiker een account heeft bij de betreffende dienst. Of als je slachtoffer bent van een phishingaanval waarbij je jouw gegevens en wachtwoord aan een aanvaller hebt gegeven.

Het NCSC raadt ook aan om wachtwoorden te vervangen wanneer de gebruiker het vermoeden heeft dat zijn computer gehackt is of is geweest. Mocht het nodig zijn om op een ander moment wachtwoorden te vervangen, dan zal de desbetreffende internetdienst daar om vragen.

Tot slot

Na tientallen jaren van wachtwoordengebruik is het tijd om op een veiliger te authentiseren. Tweefactorauthenticatie en wachtwoordmanagers vergroten de veiligheid van de gebruiker door persoonlijke gegevens beter te beschermen. De overstap naar deze middelen maken kost tijd en extra werk, maar in ruil hiervoor krijgt u een betere bescherming van uw persoonlijke gegevens. Neem het heft in eigen handen en voorkom dat kwaadwillenden toegang krijgen tot uw gegevens.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Maart 2023