Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Gebruik tweefactorauthenticatie

Factsheet FS-2015-02
versie 1.0 | 24 maart 2015

Overweeg een wachtwoordmanager, simpele wachtwoorden zijn onveilig

Accounts worden beveiligd door middel van een gebruikersnaam en wachtwoord. Deze techniek is al tientallen jaren in gebruik en is de meestgebruikte manier om toegang te krijgen tot een account. Vaak kiest een gebruiker voor simpele wachtwoorden die hij gemakkelijk onthoudt. Dit maakt het makkelijker voor kwaadwillenden om toegang te krijgen tot accounts. Wanneer een kwaadwillende toegang krijgt tot een account, kan hij zich voordoen als de eigenaar van het account en dit misbruiken.

Het NCSC adviseert gebruikers om zoveel mogelijk gebruik te maken van tweefactorauthenticatie. Ook adviseert het NCSC om sterke wachtwoorden te gebruiken en om een wachtwoordmanager te overwegen. Met deze technieken kan een kwaadwillende moeilijker toegang krijgen tot accounts en zijn gebruikers beter beschermd. Deze factsheet gaat over het gebruik van wachtwoorden [1].

Doelgroep
Deze factsheet is hoofdzakelijk bedoeld voor thuisgebruikers. Voor zakelijk gebruik van wachtwoorden wordt verwezen naar beleid van de werkgever. Daarnaast bevat dit document advies voor aanbieders van internetdiensten en werkgevers.

[1] Voor beveiligingsadviezen gerelateerd aan wachtwoorden verwijst het NCSC naar www.veiliginternetten.nl en de factsheet '10 vuistregels voor veilig internetten' van het NCSC. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-10-vuistregels-voor-veilig-internetten.html

De belangrijkste feiten

- Een gebruiker verkrijgt toegang tot een account door middel van een gebruikersnaam en wachtwoord.
- De gebruiker kiest vaak voor een simpel wachtwoord dat hij gemakkelijk onthoudt. Bij gebruik van simpele wachtwoorden kunnen kwaadwillenden toegang verkrijgen tot accounts.
- Het NCSC adviseert de gebruiker om zoveel mogelijk gebruik te maken van tweefactorauthenticatie.
- Het NCSC adviseert de gebruiker om te overwegen om een wachtwoordmanager te gebruiken.
- Het NCSC raadt aan om sterke wachtwoorden te gebruiken.

Achtergrond

Een gebruiker van internetdiensten verkrijgt vaak toegang tot een account door een gebruikersnaam en wachtwoord in te voeren. Door de vele diensten beschikt hij tegenwoordig over tientallen persoonlijke accounts waarmee hij inlogt. Voorbeelden hiervan zijn accounts voor e-mail, sociale netwerken, internetbankieren en online webwinkels. De frequentie waarmee een gebruiker deze gebruikt, hangt af van de dienst die een website aanbiedt.

Wachtwoorden zijn al tientallen jaren in gebruik en zijn nog steeds de meest voorkomende vorm van authenticatie. Door te authenticeren verifieert het systeem of de gebruiker de echte eigenaar van het account is en autoriseert het systeem de gebruiker. De laatste jaren zijn ook andere technieken ingezet als authenticatiemiddel. Een voorbeeld hiervan is biometrische gegevens waaronder vingerafdrukken.

Over het algemeen kan een gebruiker zich op drie verschillende manieren authenticeren. Deze manieren worden ook wel factoren genoemd en zijn als volgt:

- iets dat hij weet (een wachtwoord of een pincode),
- iets dat hij heeft (een telefoon of een zogenaamde token),
- iets dat hij is (een biometrisch gegeven).

Deze factsheet is tot stand gekomen in samenwerking met Logius, Rabobank, SIDN en Microsoft.

Wat is er aan de hand?

De gebruiker kiest vaak voor een wachtwoord dat hij makkelijk onthoudt. Voor gebruikers is het moeilijk om tientallen wachtwoorden te onthouden in combinatie met de website waar ze voor gebruikt worden. Dit heeft tot gevolg dat gebruikers (complexe) wachtwoorden vaak resetten. Om wachtwoorden beter te onthouden, kiezen gebruikers vaak voor wachtwoorden met de volgende kenmerken:

- Wachtwoorden hebben een korte lengte.
- Wachtwoorden zijn vaak bestaande woorden met kleine variaties. Er wordt weinig gebruik gemaakt van een reeks willekeurige tekens als wachtwoord.
- Voor meerdere accounts wordt vaak dezelfde gebruikersnaam gekozen met hetzelfde wachtwoord of een kleine aanpassing daarvan.
- Wachtwoorden worden onversleuteld opgeschreven op een stuk papier of opgeslagen op de computer of mobiele telefoon.

Wat kan er gebeuren?

Bij gebruik van simpele wachtwoorden kan een kwaadwillend persoon makkelijker toegang krijgen tot accounts. Met behulp van lijsten van veelgebruikte wachtwoorden kan hij proberen toegang te krijgen tot een account. Ook kan hij gebruik maken van technieken om een wachtwoord te achterhalen door combinaties van letters, cijfers en symbolen te proberen. Hoe korter het wachtwoord, hoe sneller een wachtwoord op deze manier gekraakt kan worden.

Wanneer een kwaadwillende toegang krijgt tot een account, kan hij zich voordoen als de eigenaar van het account en misbruik maken. Ook heeft hij 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 een Burgerservicenummer. Bovendien kan een kwaadwillende bekijken of de gebruiker het wachtwoord ook gebruikt voor andere accounts. Wanneer dit het geval is, kan hij nog meer persoonlijke informatie van de gebruiker achterhalen. Met deze gegevens kan hij vervolgens misbruik maken door 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 tijd 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.

Wat kunt u doen?

Het NCSC adviseert om zoveel mogelijk gebruik te maken van tweefactorauthenticatie en een wachtwoordmanager te overwegen. In het geval dat een gebruiker niet voor een wachtwoordmanager kiest, raadt het NCSC aan om accounts in te delen op basis van gevoeligheid en wachtwoorden te kiezen op basis van de schade die met een account veroorzaakt kan worden. Tot slot adviseert het NCSC om sterke wachtwoorden te gebruiken en een uniek wachtwoord voor elk account te kiezen.

1. Gebruik tweefactorauthenticatie

Het NCSC adviseert om waar mogelijk gebruik te maken van tweefactorauthenticatie. Een andere naam hiervoor is tweestapsverificatie. Dit bestaat uit authenticatie door middel van twee factoren uit verschillende categorieën. Een voorbeeld hiervan is het gebruik van een wachtwoord en een eenmalig te gebruiken authenticatiecode per sms. Een andere mogelijkheid is de combinatie van een vingerafdruk en een wachtwoord. In een enkel geval wordt daar een derde factor aan toegevoegd.

Tweefactorauthenticatie is veiliger dan het gebruik van enkel een wachtwoord, omdat toegang tot een account niet verkregen kan worden door enkel het achterhalen van een wachtwoord. Een kwaadwillende moet tegelijkertijd in het bezit zijn van biometrische data van de gebruiker of een fysiek element zoals een zogenaamde token of telefoon. Dit verkleint de kans dat een kwaadwillende toegang krijgt tot accounts. Voorbeelden van enkele clouddiensten tweefactorauthenticatie aanbieden zijn Google, Facebook, Twitter, LinkedIn, Dropbox, Outlook.com, DigiD en diverse banken voor internetbankieren.

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.

Advies voor aanbieders van internetdiensten

Het NCSC meent dat alle hoogwaardige internetdiensten hun gebruikers in staat moeten stellen om tweefactorauthenticatie te gebruiken. Dit is nodig om accounts beter te beveiligen. Tweefactorauthenticatie kan worden geïmplementeerd door naast de gebruikersnaam/wachtwoord combinatie een extra authenticatiemiddel toe te voegen in de vorm van een authenticatiecode via bijvoorbeeld een telefoon of een token. Zonder dit tweede middel kunnen kwaadwillenden met gerichte aanvallen gemakkelijker toegang krijgen tot een account. Grote webdiensten als Google en Facebook bieden reeds tweefactorauthenticatie aan en zetten hiermee een trend.

2. Overweeg een wachtwoordmanager

Het NCSC raadt aan om een wachtwoordmanager te overwegen. Dit is een manier om wachtwoorden digitaal te beheren. Met een wachtwoordmanager is het mogelijk om wachtwoorden versleuteld op te slaan. Om toegang te krijgen tot de wachtwoordmanager

	Geen wachtwoordmanager	Wachtwoordmanager	Online wachtwoordmanager	Offline wachtwoordmanager
Voordeel	De gebruiker is niet afhankelijk van de beveiliging van een systeem.	De gebruiker kan zeer complexe wachtwoorden gebruiken en voor elk account een ander wachtwoord instellen. Hij hoeft slechts één wachtwoord te onthouden.	Het wachtwoordbeheer en synchronisatie zijn eenvoudig.	De gebruiker heeft zelf de controle over het beheer van zijn wachtwoorden.
Nadeel	De gebruiker zal al zijn wachtwoorden zelf moeten onthouden.	Compromittatie van de wachtwoordmanager leidt tot compromittatie van alle wachtwoorden.	De gebruiker zal de clouddienst moeten vertrouwen.	De gebruiker zal wachtwoorden handmatig moeten synchroniseren en de versleutelingstechniek moeten vertrouwen.

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 wachtwoordmanager waardoor de gebruiker ze niet meer hoeft te onthouden. Hij kan deze wachtwoorden op elk moment opvragen bij de wachtwoordmanager. Hierdoor kan hij zeer complexe wachtwoorden gebruiken en kan hij voor elk account een ander wachtwoord instellen. Een nadeel is dat alle wachtwoorden op dezelfde plek worden bewaard. Wanneer de wachtwoordmanager wordt gecompromitteerd, krijgt kwaadwillende toegang tot alle wachtwoorden van de gebruiker.

Er zijn twee typen wachtwoordmanagers: online en offline wachtwoordmanagers. Een online wachtwoordmanager is handiger, een offline wachtwoordmanager is veiliger.

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 wijzigen is daardoor maar op één apparaat nodig. Voorbeelden van veelgebruikte online wachtwoordmanagers zijn LastPass en Dashlane[2].

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 handmatig moeten aanpassen, omdat de wachtwoordmanagers niet automatisch synchroniseren. Voorbeelden van offline wachtwoordmanagers zijn Keepass en 1Password[3].

Met deze offline wachtwoordmanagers is het ook mogelijk om het versleutelde bestand met wachtwoorden op te slaan bij een clouddienst als Dropbox of iCloud. 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 aan online als offline wachtwoordmanagers zitten voor- en nadelen. Een voordeel van een online wachtwoordmanager is dat het beheer van wachtwoorden makkelijk is en dat 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 met de versleutelde wachtwoorden wordt omgegaan in de cloud. Wanneer een kwaadwillende een kwetsbaarheid vindt in deze dienst, is het mogelijk dat alle wachtwoorden van alle gebruikers op straat komen liggen.

Een voordeel van een offline wachtwoordmanager is dat de gebruiker zelf de controle heeft over het beheer van zijn wachtwoorden. Hij slaat zijn wachtwoorden lokaal op en is niet afhankelijk van de beveiliging van een clouddienst. Hij is dan ook zelf verantwoordelijk voor de beveiliging van de plek waar hij zijn wachtwoorden opslaat. 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 inspanning.

[2] Deze wachtwoordmanagers worden aangeraden door de consumentenbond: http://www.consumentenbond.nl/veilig-online/extra/test-wachtwoordmanagers/

[3] KeePass wordt geadviseerd door de consumentenbond: http://www.consumentenbond.nl/veilig-online/extra/test-wachtwoordmanagers/, 1Password wordt geadviseerd door veiliginternetten.nl: https://veiliginternetten.nl/themes/situatie/ik-kan-mijn-wachtwoord-niet-onthouden/

Handelingsperspectief:

1. Het NCSC adviseert om gebruik te maken van tweefactorauthenticatie waar mogelijk.
2. Het NCSC raadt aan om te overwegen om een wachtwoordmanager te gebruiken voor het beheer van wachtwoorden. U bepaalt zelf of u voor een online of offline wachtwoordmanager kiest.
3. Als u kiest om geen wachtwoordmanager te gebruiken, raadt het NCSC aan om accounts in te delen in categorieën op basis van risico's die misbruikt van accounts met zich meebrengen.
4. Het NCSC adviseert om sterke wachtwoorden te gebruiken en het herhalen van wachtwoorden voor verschillende accounts te voorkomen.

In beide gevallen zal de gebruiker het hoofdwachtwoord van de wachtwoordmanager moeten onthouden. Wanneer hij dit vergeet, heeft hij op dat moment geen toegang meer tot al zijn accounts en zal hij deze moeten laten resetten. Om dit te voorkomen, kan hij ervoor kiezen om het hoofdwachtwoord op papier te schrijven en dit op een veilige plek te bewaren, bijvoorbeeld in een kluis.

Tweefactorauthenticatie en wachtwoordmanagers op de werkplek

Het NCSC adviseert werkgevers om tweefactorauthenticatie te implementeren. Tweefactorauthenticatie, om toegang te krijgen tot de computer op de werkplek, kan worden geïmplementeerd door werknemers te laten inloggen met behulp van een wachtwoord en een token. Dit verkleint de kans dat onbevoegden toegang krijgen tot computers van uw werknemers.

Ook adviseert het NCSC werkgevers om na te denken over een geschikte vorm van authenticatie voor accounts gerelateerd aan de werkplek. Wanneer een werknemer beschikt over meerdere accounts, bestaat het risico dat werknemers hun wachtwoorden voor de werkplek willen opslaan in online wachtwoordmanagers, in wachtwoordmanagers op hun privé computer thuis of dat zij wachtwoorden op een onveilige plek op papier bewaren.

De werkgevers zou bijvoorbeeld een offline wachtwoordmanager kunnen aanbieden voor op de werkplek. Een andere mogelijkheid is om single sign-on te implementeren.

3. Deel accounts in op basis van gevoeligheid

Het NCSC adviseert gebruikers die om welke reden dan ook geen wachtwoordmanager willen gebruiken accounts in te delen op basis van de risico's die een hack van het account met zich meebrengt. Dit gebeurt door ze op te delen in verschillende categorieën met tenminste de volgende twee categorieën: accounts met een lage waarde en accounts met een hoge waarde[4]. Tot de eerste categorie behoren informatieve websites waar weinig tot geen persoonlijke gegevens zijn opgeslagen. Het effect dat een hack heeft op deze categorie accounts is kleiner. De gebruiker zal hier zelf de sterkte van wachtwoorden moeten afwegen. Hier wordt aangeraden om unieke wachtwoorden te gebruiken. De tweede categorie bestaat uit accounts die belangrijke persoonlijke gegevens bevatten waarmee bijvoorbeeld fraude kan worden gepleegd. Voorbeelden zijn e-mailaccounts en accounts van websites van banken. Hierbij is het belangrijk dat de gebruiker een lang en uniek wachtwoord gebruikt. Een sterk wachtwoord voor deze accounts is van groot belang om de kans op fraude te verkleinen.

4. Kies sterke wachtwoorden

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

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

Het is lastig om een goed en sterk wachtwoord te kiezen. Toch is het belangrijk dat wachtwoorden sterk zijn en bovendien het hoofdwachtwoord van de wachtwoordmanager goed te onthouden is. Het NCSC is van mening dat wanneer de gebruiker een keuze moet maken tussen soorten wachtwoorden het beter is om lange wachtwoorden dan complexe wachtwoorden te kiezen. ECP heeft een module gemaakt die test hoelang het duurt om een wachtwoord te kraken en geeft daarmee een indicatie over de sterkte van een wachtwoord[5]. Het is niet aan te raden om de sterke 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 hij bijvoorbeeld kiezen voor een wachtzin met een lengte van 30 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 of leestekens 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 hij laten

[4] Deze methode is gebaseerd op: http://research.microsoft.com/pubs/217510/passwordportfolios.pdf

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

genereren door de wachtwoordmanager. De veiligste manier is om dit te laten doen door een offline wachtwoordmanager.

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 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. Een andere situatie is wanneer de gebruiker het vermoeden heeft dat zijn computer gehackt is of is geweest. Het NCSC raadt aan om van belangrijke accounts periodiek het wachtwoord te vervangen indien geen gebruik wordt gemaakt van 2-factor authenticatie. Mocht het nodig zijn om op een ander moment wachtwoorden te vervangen, dan zal de desbetreffende internetdienst daar om vragen.

Tot slot:

Na enkele tientallen jaren van wachtwoordengebruik is het tijd voor een stap vooruit. Tweefactorauthenticatie en wachtwoordmanagers vergroten de veiligheid van de gebruiker door persoonlijke gegevens beter te beschermen. De overstap naar deze nieuwe middelen kost enige tijd, maar in ruil hiervoor krijgt u een betere bescherming van uw persoonlijke gegevens. Neem het heft zelf in handen en voorkom dat kwaadwillenden toegang krijgen tot uw gegevens.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55
Publicatienr: FS-2015-02 1.0 | Aan deze informatie kunnen geen rechten worden ontleend.