Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Volwassen authenticeren

Gebruik veilige middelen voor authenticatie

Factsheet FS-2022-01 | versie 1.2 | April 2022

Authenticatie is de techniek waarmee een systeem de identiteit van een gebruiker vaststelt. Na een succesvolle authenticatie krijgt de gebruiker toegang tot accounts en systemen binnen een organisatie. Het meest bekende voorbeeld van authenticatie is inloggen met een gebruikersnaam en wachtwoord. Dit is echter ook de meest onveilige methode van authenticatie.

Wanneer een kwaadwillende de inloggegevens van een legitieme gebruiker achterhaalt, kan hij ook de accounts en systemen van de organisatie binnendringen. Er zijn veel manieren waarop hij dit met weinig moeite kan doen.

Sterkere authenticatiemethoden bieden meer bescherming tegen dergelijke aanvallen. Voorbeelden hiervan zijn tweefactorauthenticatie en de FIDO2-standaard van de FIDO Alliance. In deze factsheet leest u welke afwegingen u kunt maken bij het bepalen van een geschikte authenticatiemethode voor de accounts en systemen binnen uw organisatie.

Doelgroep

CISO’s, identieits- en toegangsbeheerders, securitymanagers

Aan deze factsheet hebben bijgedragen:

FI-ISAC, Rabobank, de Volksbank

Achtergrond

Authenticatie is de techniek waarmee een systeem kan vaststellen wie een gebruiker is. Hiermee krijgt een gebruiker toegang tot gegevens of systemen. Authenticatie is een onderdeel van identiteits- en toegangsbeheer en wordt in toepassingen aangevuld met autorisatie. De relatie tussen die twee is dat authenticatie de identiteit van een gebruiker kenbaar maakt. Dat gebeurt bij autorisatie niet. Autorisatie gaat over het toewijzen van bepaalde rechten binnen het systeem voor de gebruiker nadat deze succesvol is geauthenticeerd.

Accounts en systemen kunnen door verschillende typen authenticatiemiddelen beveiligd worden. Doorgaans worden deze als volgt gecategoriseerd:

- Iets wat men weet (bijvoorbeeld gebruikersnaam + wachtwoord)
- Iets wat men is (biometrische gegevens, bijvoorbeeld een irisscan)
- Iets wat men heeft (bijvoorbeeld een telefoon of zogenaamde token)

Gebruikersgemak en veiligheid

Gebruikersgemak speelt een grote rol bij het beveiligen van accounts en systemen. Een niet-gebruiksvriendelijk authenticatiemiddel zorgt ervoor dat eindgebruikers op zoek gaan naar alternatieven en zo mogelijk de beveiliging omzeilen. Daarmee daalt de effectieviteit van de geïmplementeerde veiligheidsmaatregel. Bijvoorbeeld: een werknemer moet regelmatig een wachtwoord aanpassen. Een verouderde regel die vroeger nog werd aangeraden, maar in de praktijk niet goed werkt. Gebruikers kiezen makkelijke wachtwoorden en passen vaak slechts een enkel teken in het wachtwoord aan. Ook komt het regelmatig voor dat een wachtwoord voor verschillende systemen gebruikt wordt.

Wat is er aan de hand?

Kwaadwillenden die toegang willen krijgen tot systemen kunnen zich richten op het doorbreken van het authenticatiemechanisme. De aanvalstechnieken die gebruikt worden zijn steeds toegankelijker en gemakkelijker om uit te voeren. Daarmee neemt de kans op deze ongeautoriseerde inlogpogingen toe. In tabel 1 worden veelvoorkomende aanvalstechnieken met betrekking tot ongeautoriseerde inlogpogingen toegelicht.

Accounts met verhoogde rechten binnen een systeem, zoals beheerdersaccounts, zijn steeds vaker het doelwit van aanvallen. Zij hebben vaak toegang (autorisatie) tot gevoelige informatie en zijn daardoor vanwege financieel- en informatief gemotiveerde redenen een interessant doelwit. Een kwaadwillende kan bijvoorbeeld ransomware installeren op de voor de beheerder toegankelijke data en systemen. De impact van een dergelijke aanval is groot.

Gezien deze ontwikkeling is het extra belangrijk om accounts op een gepaste manier te beveiligen. Het Cybersecuritybeeld Nederland 2021 onderschrijft het belang van goede authenticatie en laat zien dat het dreigingsniveau voor zwakke authenticatie hoog is.[1]

Tabel 1 **Dreigingen**

Dreiging	**Omschrijving met betrekking tot authenticatie**
Credential phishing	Een aanval waarbij de kwaadwillende zich voordoet als betrouwbare bron om inloggegevens te vergaren. Vorm van social engineering.
Brute-force aanvallen	Het kraken van inloggegevens door alle mogelijkheden af te gaan.
Diefstal uit datalekken	Wanneer informatie gelekt is kunnen deze gegevens gebruikt worden om automatische inlogpogingen te faciliteren.
Dictionary attacks	Een brute-force methode waarin inloggegevens vergaard worden door vaak gebruikte wachtwoorden en variaties daarvan (automatisch) in te voeren.
Social engineering	Het vergaren van inloggegevens doormiddel van sociale relaties of manipulatie.
Key logging	Malware die de aanslagen op het toetsenbord opneemt en zo inloggegevens vergaart.

Verschillen in authenticatie

Niet alle typen authenticatie zijn even weerbaar tegen bovenstaande dreigingen. Zo is authenticatie met alleen een gebruikersnaam en wachtwoord het minst veilig van de benoemde authenticatiemethodes. Deze vorm van authenticatie is zeer gevoelig voor alle dreigingen in tabel 1. Authenticatie waarbij een tweede veiligheidslaag is geïmplementeerd naast het traditionele gebruikersnaam en wachtwoord verhoogt de beveiliging van accounts en systemen aanzienlijk. Wanneer er twee verschillende categorieën (iets wat je bent, hebt of weet) ingezet worden om te authenticeren spreken we van tweefactorauthenticatie (2FA).

Niet alle vormen van 2FA zijn hetzelfde. In het algemeen is 2FA waarbij een sms of e-mail met een eenmalige code wordt verstuurd na het invoeren van gebruikersnaam en wachtwoord de minst veilige vorm van 2FA. Dit komt omdat deze methode gelegenheid biedt tot phishing en zogenoemde man-in-the-middle aanvallen. Bij een man-in-the-middle aanval onderschept de kwaadwillende het verkeer tussen communicerende partijen. Dat verkeer kan dus ook het wachtwoord en de code van de tweede authenticatiestap zijn.

Het gebruik van biometrische gegevens als tweede veiligheidslaag is minder gevoelig voor de genoemde dreigingen, maar is onderhevig aan wetten en regels omtrent privacy zoals de Algemene Verordening Gegevensbescherming (AVG). Deze maatregel moet dus passen binnen de

[1] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

organisatie. Daarnaast zijn tokens ook een veiligere vorm van 2FA. Er kan onderscheid gemaakt worden tussen software tokens (bijv. een one-time-password (OTP) in een app) en hardware tokens (bijv. een smartcard of usb-sleutel). Ondanks de hoge mate van beveiliging beschermen niet alle tokens tegen phishing. Een standaard van de FIDO Alliance genaamd FIDO2 is wel bestand tegen phishing.[2] Tokens die deze standaard implementeren, bieden daardoor de meest uitgebreide beveiliging voor authenticatie tot op heden.

Overige factor

Een andere factor die de beveiliging van authenticatie beïnvloedt is gebruikersgemak. Tabel 2 is een overzicht van de verschillende typen authenticatie, de voor- en nadelen daarvan en een beoordeling over de gebruiksvriendelijkheid van de maatregel.

Tabel 2 **Type authenticatie**

Authenticatie	**Voordelen**	**Nadelen**
Gebruikersnaam en wachtwoord	Gangbaar voor ontwikkelaars.	Gevoelig voor alle dreigingen in tabel 1. Niet gebruiksvriendelijk.
Tweefactorauthenticatie met sms of e-mail	Veiliger dan enkel gebruikersnaam en wachtwoord.	Gevoelig voor man-in-the-middle-aanvallen, phishing en social engineering. Niet gebruiksvriendelijk.
Biometrie	Sterke vorm van beveiliging.	Privacy- en ethische vraagstukken en/of regels.
Softwaretokens	Gemakkelijke en veilige vorm van authenticatie, daardoor gebruiksvriendelijk.	Niet volledig weerbaar tegen phishing. Softwaretokens kunnen eenvoudiger gecompromitered worden dan hardwaretokens.
Hardwaretokens	Gemakkelijke en veilige vorm van authenticatie, daardoor gebruiksvriendelijk.	Niet volledig bestand tegen phishing. Hardware tokens kunnen kwijt raken.
Phishing-resistente authenticatie (WebAuthn)	Meest veilige vorm van authenticatie, phishing-resistent en gebruiksvriendelijk.	Wanneer browsers niet up-to-date zijn zullen zij wellicht FIDO2 nog niet ondersteunen. Hardware tokens kunnen kwijt raken.

[2] Deze factsheet refereert met phishing aan grootschalige bulk-phishing. Spear-phishing in combinatie met DNS-kaping wordt in de context van deze factsheet buiten beschouwing gelaten.

WebAuthn

FIDO2 is een open standaard van de FIDO (Fast Identity Online) alliance. De standaard bestaat uit WebAuthn, een WebAPI en het Client to Authenticator Protocol (CTAP). FIDO2 is gebaseerd op publiekesleutelcryptografie en biedt een hoge mate van beveiliging. Dit komt omdat de inlog-gegevens uniek zijn voor elk systeem, en enkel daar te gebruiken zijn. Zo wordt hergebruik van een onderschepte authenticatie door een kwaadwillende tussen gebruiker en het legitieme systeem onmogelijk. De privésleutel verlaat het geregistreerde apparaat niet en wordt niet opgeslagen op een server. Privésleutels kunnen alleen individueel uitlekken, dit maakt mogelijke aanvallen minder schaalbaar. Bovendien, omdat alleen publieke sleutels uitlekken bij een traditioneel datalek is er geen risico op misbruik. Tot slot is de opgeslagen publieke sleutel uniek en daardoor niet traceerbaar.

Wat kan er gebeuren?

Een kwaadwillende kan middels een van de genoemde dreigingen in tabel 1 toegang krijgen tot uw accounts en systemen. De kans op ongewenste toegang is groter wanneer er sprake is van minder veilige authenticatiemethoden. De impact van een aanval is groter wanneer een legitieme gebruiker autorisatie heeft tot gevoelige informatie. Dat komt omdat een kwaadwillende na een succesvolle aanval volledige toegang heeft tot het systeem met alle toegangsrechten van het account waarop is ingebroken. Enkele voorbeelden van impact zijn:

- De aanvaller kan vertrouwelijke informatie stelen.
- De aanvaller kan uw bedrijfsvoering verstoren als data cryptografisch versleuteld wordt en er een geldbedrag betaalt moet worden om weer hier weer toegang tot te krijgen. Dit wordt ransomware genoemd. Bij een gebrek aan recente back-ups die hersteld kunnen worden is de kans groot dat de data voorgoed weg is.
- Zelfs een aanval op een account met weinig toegangsrechten kan ook gebruikt worden door een kwaadwillende om bij gevoelige informatie te komen. Vanuit het account met weinig toegangsrechten kan de kwaadwillende namelijk opnieuw scannen op kwetsbaarheden binnen een netwerk. Wanneer dit niet wordt opgemerkt kan hij gebruik maken van deze kwetsbaarheden tot hij bij de gewenste informatie uitkomt.

Advies

Beveilig uw accounts op een manier die past bij de gevoeligheid van de gegevens en middelen waar deze toegang toe bieden. Maak hierbij onderscheid tussen verschillende accounts op basis van het bijbehorende risico. High-impact accounts (bijvoorbeeld beheerdersaccounts) vereisen een andere mate van beveiliging dan low-impact accounts (bijvoorbeeld gastaccounts). Bepaal het risico voor de accounts binnen uw organisatie en beveilig deze op een gepaste manier. Het volwassenheidsmodel voor authenticatie helpt u bij het bepalen van de gepaste beveiliging. Over het algemeen blijkt dat niveau 0 onvoldoende bescherming biedt.

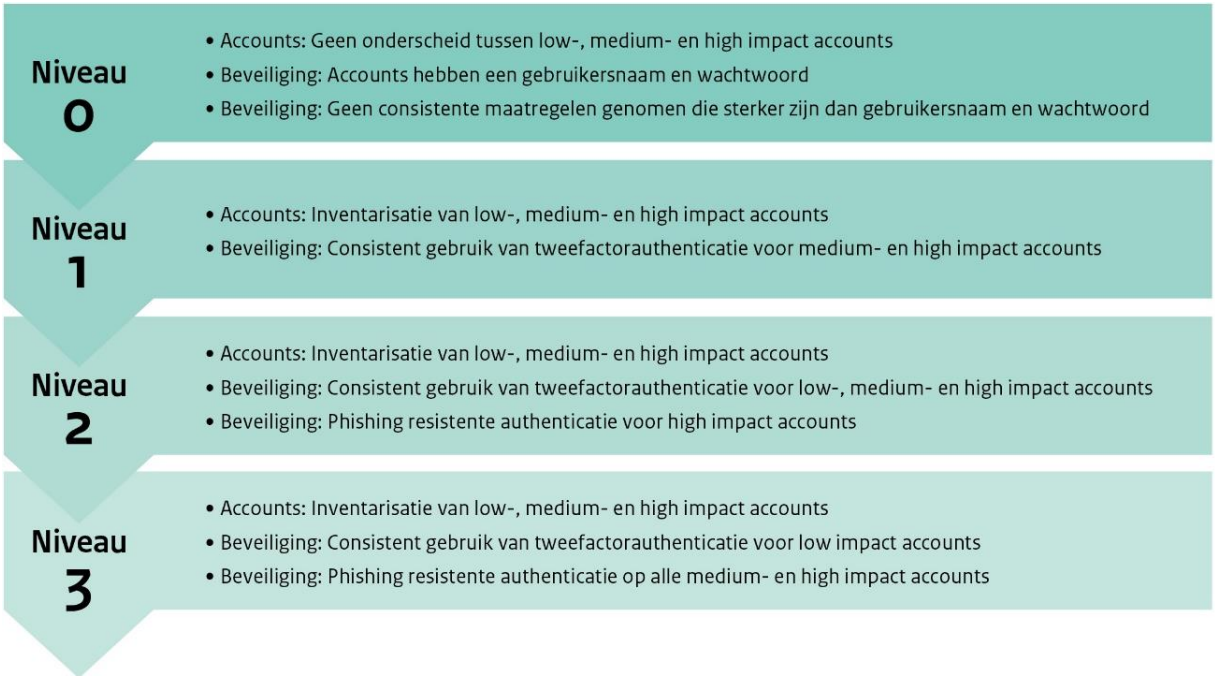
Mitigerende maatregelen

Naast de gepaste beveiliging zijn er ook mitigerende maatregelen die u kunt toepassen om de kans op ongeautoriseerde inlogpogingen te verminderen. Deze maatregelen kunnen ervoor zorgen dat een organisatie die niet aan alle eisen voor een bepaald volwassenheidsniveau voldoet, de weerbaarheid alsnog (tijdelijk) op een acceptabel niveau kan krijgen.

- Positie van uw interne- en externe toegangspunten op het netwerk: De positie van accounts en systemen in het netwerk kan het risico op ongeautoriseerde inlogpogingen veranderen, waarbij bijvoorbeeld de kans op ongeautoriseerde inlogpogingen op het interne netwerk kleiner is.
- Monitoring op toegangssystemen: Wanneer er sprake is van monitoring op een toegangssysteem wordt er actief gekeken naar verdachte inlogpogingen. De kans op een ongeautoriseerde inlogpoging die niet wordt opgemerkt is daardoor kleiner.[3]
- Een maximaal toegestaan aantal inlogpogingen per tijdseenheid: Door een maximaal aantal inlogpogingen per tijdseenheid te hanteren is de kans op een succesvolle aanval waarbij geen interactie nodig is met de legitieme gebruiker (brute-force) en de kans op een Denial-of-Service (DoS) kleiner. Beperk de inlogpogingen van de specifieke client, niet op basis van het account.

Het NCSC adviseert u om met behulp van het volwassenheidsmodel voor authenticatie een passende authenticatiebeveiliging in te richten binnen de organisatie. Mitigerende maatregelen verminderen daarbij het risico en zorgen voor extra beveiliging.

Volwassenheidsmodel



Handelingsperspectief

Het NCSC adviseert u om op basis van een risicobeoordeling uw accounts in te delen in low-medium- en high impact accounts. Vervolgens kunt u de accounts met behulp van het

[3] Monitoring is een detectiemethode en biedt daardoor niet dezelfde mate van beveiliging als het implementeren van de juiste authenticatiemethode.

volwassenheidsmodel voor authenticatie op een gepaste manier gaan beveiligen. Hierbij kan onderscheid gemaakt worden tussen de implementatie van tweefactorauthenticatie (2FA) en phishing-resistente authenticatie. Tot slot adviseert het NCSC om aanvullende mitigerende maatregelen te implementeren.

Implementeer tweefactorauthenticatie

De precieze manier waarop 2FA kan worden ingesteld verschilt per applicatie en systeem. Ga na bij uw IT-beheerder of en hoe implementatie van 2FA mogelijk is. Zo bieden bijvoorbeeld veel clouddiensten zoals Google, Outlook en Dropbox 2FA aan. Er zijn mogelijk ook wettelijke eisen of normenkaders die 2FA voor uw organisatie verplichten.

Er zijn nog een aantal andere dingen waar rekening mee gehouden moet worden bij de implementatie van 2FA. 2FA moet gereset kunnen worden wanneer bijvoorbeeld een telefoon of token kwijtgeraakt is. Herstelsleutels dienen op een andere plek bewaard te worden dan het wachtwoord**.**

Wanneer uw organisatie een publieke organisatie betreft waarbij met DigiD ingelogd kan worden, moet u zich houden aan de eIDAS-verordening. Tot slot moet uw organisatie de privacywetgeving in acht nemen bij het implementeren van een veiligheidsmaatregel wanneer er gewerkt wordt met persoonsgegevens.

Implementeer phishing-resistente authenticatie

Ondanks dat de standaard nog niet overal verspreid is, groeit het aantal FIDO-compatibele platformen en browsers snel. Een overzicht van de browsers en platforms waar FIDO2 wordt ondersteund is te vinden op de website van de FIDO Alliance.[4] U kunt FIDO2 onder andere toepassen op applicaties in Google Chrome, Microsoft Edge en Windows 10. Kijk op de website van FIDO Alliance hoe u aan de slag kunt gaan met het implementeren en inzetten van FIDO2.[5]

Neem aanvullende maatregelen

Richt monitoring en logging in. Monitoring en logging vindt plaats om onverwacht gebruik te detecteren. Zie ook onze factsheet 'SOC inrichten, begin klein'.[6]

Maak een inventarisatie van interne- en externe toegangspunten op uw netwerk, zodat u weet waar het risico op ongeautoriseerde inlogpogingen het hoogst is. Dit is over het algemeen op de externe toegangspunten in uw netwerk. Desalniettemin blijft er ook op uw interne netwerk altijd een risico aanwezig, bijvoorbeeld dat van ontevreden medewerkers.

Stel bovendien een maximaal aantal toegestane inlogpogingen per tijdseenheid in voor alle clients. Het is daarnaast gewenst dat medewerkers zicht kunnen hebben op hun inloggeschiedenis. Zo kunnen verdachte activiteiten sneller opgemerkt en gerapporteerd worden.

[4] FIDO2: Web Authentication (WebAuthn) - FIDO Alliance

[5] Implementation & Deployment - Getting FIDO up & running (fidoalliance.org)

[6] Factsheet SOC inrichten: begin klein | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl)

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

April 2022