Veiliger inloggen met de Reset Authenticator

Met de Reset Authenticator kunt u ongewenste personen buitensluiten, zelfs als ze het wachtwoord van een gebruiker hebben. Door middel van Two-Factor Authentication creëert Reset een extra beveiligingslaag met een device die een gebruiker bij zich heeft. Hiermee kunnen uw werknemers veiliger inloggen en verminderen we het risico dat een kwaadwillende (hacker of werknemer) misbruik van uw bedrijfsdata kan maken.

Wat is Two-Factor Authentication?

Two-Factor Authentication, vaak afgekort als 2FA, is een extra laag van bescherming voor een gebruikerswachtwoord. Het combineert een wachtwoord met een tweede factor, zoals bijvoorbeeld een smartphone (iets wat ook toebedeelt kan worden aan een persoon). Hiermee kan een systeem vaststellen dat een gebruiker daadwerkelijk is wie hij claimt te zijn door twee van deze factoren te toetsen. Dankzij 2FA moet een hacker die uw wachtwoord heeft, ook nog iets bezitten om toegang te krijgen tot uw account.

Veel grote websites hebben de mogelijkheid om 2FA in te schakelen al beschikbaar gesteld bij hun Beveiligingsinstellingen. Toch wordt het op de werkvloer nog niet voldoende of structureel gebruikt, terwijl inloggen zonder Two-Factor Authentication voor organisaties grote risico's oplevert en het 'kwijtraken' van privacygevoelige informatie altijd consequenties heeft. Vooral nu sinds 1 januari 2016 de Meldplicht Datalekken geldt in Nederland.

Reset Authenticator voor RDP

Reset biedt een veilige en mobiele oplossing aan om het inloggen via het Remote Desktop Protocol (RDP) te voorzien van Two-Factor Authentication. Met de Reset Authenticator krijgen uw werknemers een extra factor om in te loggen: een One-Time Password (OTP) dat 30 seconden geldig is en afgelezen kan worden met een smartphone, tablet of wearable.

reset
Innovatie
Lab

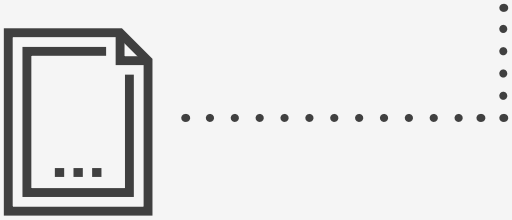
Hoe werkt Two-Factor Authentication?

One-Time Password (OTP)

Via een mobiel apparaat wordt een OTP verstrekt aan de gebruiker.

Gebruikerswachtwoord + OTP

De gebruiker combineert zijn standaard wachtwoord met de verstrekte OTP.



Toegang tot bedrijfsdata

Bij succesvolle autorisatie wordt toegang verleend tot het systeem.

OTP
984265

One-Time Password (OTP)

Een One-Time Password (OTP) is een eenmalig wachtwoord dat bij elk gebruik wijzigt. De OTP's worden willekeurig gegenereerd, zodat deze niet kunnen worden voorspeld of hergebruikt.

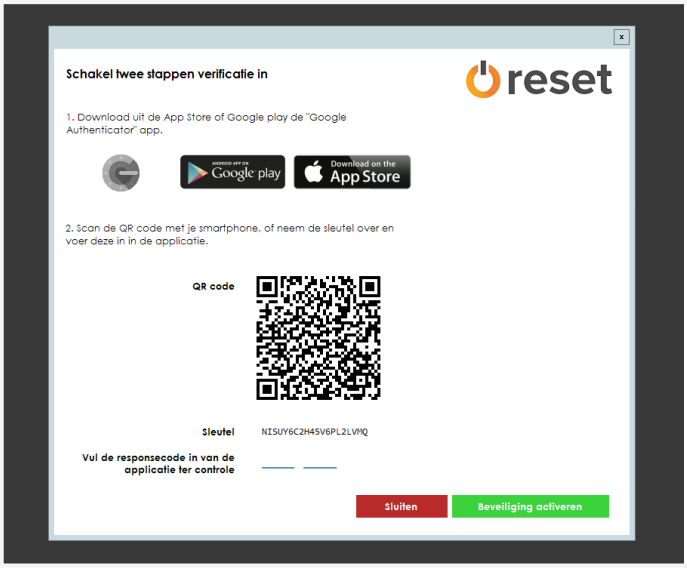
Waarom een enkel wachtwoord niet meer volstaat

Bij veel besturingssystemen, applicaties en platformen vertrouwen gebruikers nog steeds op een enkel wachtwoord om hun identiteit en bedrijfsgegevens te beschermen. Deze vorm van autoriseren wordt ook wel Single-Factor Authentication genoemd. Deze inlogmethode is niet alleen sterk verouderd, maar kan als een zwakke plek beschouwd worden binnen uw organisatie.

- Een enkel wachtwoord is sterk afhankelijk van de kwaliteit van het gekozen wachtwoord. Gebruikers hebben echter de neiging om steeds dezelfde wachtwoorden te hanteren. Een groot risico, zeker wanneer ze hetzelfde wachtwoord gebruiken voor e-mail of online bankieren.
- Accounts worden steeds vaker gehackt en gebruikersgegevens buitgemaakt. Zonder een extra factor om de identiteit van een gebruiker te bevestigen, kan een hacker met alleen het wachtwoord inloggen.
- Hackers gebruiken steeds inventievere methodes om aan wachtwoorden te komen. Zo kunnen ze bijvoorbeeld op afstand meekijken met gebruikers die inloggen en hierbij ook de toetsaanslagen lezen. Ook komen er steeds meer databases voor hackers beschikbaar waarin veelgebruikte wachtwoorden opgeslagen staan. Hiermee wordt het nog gemakkelijker voor hackers om wachtwoorden te kraken.

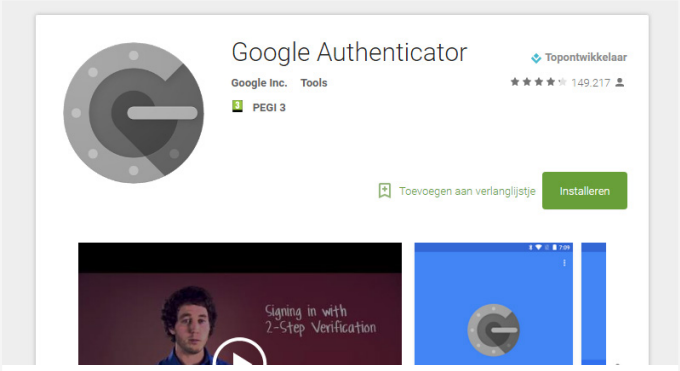
Wat heeft u nodig voor Two-Factor Authentication?

Bij het aanzetten van Two-Factor Authentication voor een gebruiker wordt er een ‘shared secret’ gegenereerd. Deze vormt, in combinatie met tijd, de basis van een One-Time Password. Om aan een OTP te komen zijn er diverse Authenticator-apps die het ‘shared secret’ omzetten in een 30-seconden geldige OTP. Reset adviseert het gebruik van Google Authenticator (beschikbaar voor Android- en iOS) in combinatie met een mobiel apparaat.



Reset Authenticator

Met de Reset Authenticator bieden we Two-Factor Authentication aan voor het Remote Desktop Protocol. Deze eigen ontwikkelde software zorgt ervoor dat er naast een gebruikersnaam en wachtwoord ook een One-Time Password (OTP) vereist is om in te loggen. Pas na een correcte combinatie van deze gegevens wordt er toegang tot het systeem verleend.



Google Authenticator

Om een OTP te genereren en te kunnen verschaffen aan uw werknemers gebruikt Reset de Google Authenticator. Met deze applicatie verschaft u niet alleen op veilige wijze OTP’s, maar kunt u ook meerdere sleutels op een overzichtelijke manier bewaren.

Mobiel apparaat

De keuze voor mobiele apparaten (smartphones, tablets of wearables) is logisch: deze zijn niet meer weg te denken op de werkvloer en waarschijnlijk hebben uw werknemers ze reeds in bezit. Daarnaast is het moeilijker om een mobiel apparaat te vergeten of kwijt te raken dan een (extra) hardware token.

reset Innovatie Lab

Binnen het Innovatielab ontwikkelt ons R&D-team nieuwe diensten en technieken om innovatie toegankelijk en betaalbaar te maken. Daarnaast is het de ‘innovation playground’ van Reset om creatieve oplossingen te realiseren. Zo blijven we altijd vooruitkijken.

Meer weten over security?

Heeft u vragen of wilt u meer informatie over security? Reset biedt professional services, managed services en technologie voor het beveiligen van uw ICT-infrastructuur. Ook kunnen we uw organisatie begeleiden bij het uitvoeren van uw eigen beveiligingsmaatregelen, zodat we samen uw cybersecurity kunnen verbeteren.

Kijk op reset.nl voor meer informatie.