CSL Multifactorauthenticatie

Wat is Multifactorauthenticatie (MFA)?

MFA is een authenticatieproces gebaseerd op twee verificatiemethodes om de identiteit van de gebruiker te verifiëren. Hierdoor wordt de toegangscontrole van een systeem aangescherpt.

Deze vorm van authenticatie biedt bescherming tegen phishing, social engineering en brute-force attacks. Bovendien kan men via MFA inloggegevens beveiligen tegen aanvallers die misbruik maken van zwakke of gestolen toegangsgegevens.

Waarom is MFA belangrijk?

MFA is een essentieel onderdeel van een ***Zero Trust-beveiligingsmodel***. Gebruikers die toegang willen tot bepaalde gegevens, moeten bevestigen dat zij zijn wie zij zeggen te zijn. MFA biedt bescherming tegen heel wat beveiligingsbedreigingen gericht op wachtwoorden en accounts van gebruikers, zoals die hierboven vermeld.

Wanneer een aanvaller op afstand een computer kan binnendringen via de internetverbinding van een gebruiker, kan hij/zij toegang krijgen tot het wachtwoord van deze gebruiker en tot een tweede vorm van authenticatie als beide via hetzelfde kanaal worden verstuurd.

Het is evenwel niet mogelijk voor aanvallers op afstand om de identiteit van een gebruiker te stelen (om zo toegang te krijgen tot in toepassingen opgeslagen informatie) zonder in het bezit te zijn van het fysieke apparaat van die persoon.

De integratie van MFA maakt het voor aanvallers onmogelijk om toegang te krijgen tot privé-accounts zonder te beschikken over het fysieke apparaat nodig voor het voltooien van de tweede authenticatiefactor.

Welke type MFA gebruikt CSL?

CSL gebruikt tijdfactorauthenticatie, ook wel Time-Based One Time Password (TOTP) genoemd. De TOTP MFA-methode genereert een code op tijd gebaseerde intervallen die de gebruiker moet invoeren om in te loggen. De door de authenticator-apps of via SMS/e-mail gegeneerde toegangscode vervalt na een bepaalde periode. Wanneer de gebruiker een volgende keer inlogt op zijn/haar account wordt een nieuwe code gegenereerd. TOTP is onderdeel van de Open Authentication (OAUTH) beveiligingsarchitectuur.

CSL DualCom Ltd
Building 4, Croxley Park
Hatters Lane, Watford
WD18 8YF, United Kingdom

T +44 (0) 1895 474 474
E sales@csl-group.com
W www.csl-group.com
@CSLGroupLtd

Registered in England No. 03155883
CSL2136V1 0608021

CSL heeft tijdfactorauthenticatie met OTP, e-mail en SMS geïmplementeerd. Hieronder vindt u een lijst met veel gebruikte, door CSL goedgekeurde authenticator-apps:

- Free OTP
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile
- IBM Security Verify

Hoe werkt het?

1. Voer uw gebruikersnaam en wachtwoord in op CSL Live zoals gewoonlijk.
2. U ontvangt een code via uw Authenticator-app, -programma, e-mail of SMS.
3. Voer de code in CSL Live in.
4. U bent nu veilig ingelogd.

Welke sectoren maken gebruik van MFA?

Meerdere sectoren zetten endpoint-beveiliging steeds hoger op hun agenda. Ongeacht de gebruikte toepassingen, het beschermen van inloggegevens is van kapitaal belang om de veiligheid van de hele sector te waarborgen.

Detailhandel 

In de sector met de meeste tewerkstellingen komen aanvallen op afstand vaak voor en zijn ze moeilijk te voorkomen. Bovendien worden beveiligingsoplossingen steeds belangrijker voor de detailhandel nu de informatietechnologie zich aanpast aan een omgeving zonder perimeter. MFA biedt bedrijven in de detailhandel een zeker gemoedsrust door hen in staat te stellen de identiteit te verifiëren van gebruikers die via externe computers en persoonlijke mobiele apparaten verbinding maken met hun netwerk.

Banksector 

Banken maken gebruik van MFA om zich te beschermen tegen de vele hackpogingen op zowel hun eigen interne systemen als op die van hun klanten. MFA heeft al vele grootbanken geholpen hun weerbaarheid tegen dergelijke aanvallen te verbeteren.

Voor banken is het heel belangrijk om te weten welke gebruikers en apparaten op een bepaald moment toegang hebben tot hun systemen. De banksector kan door middel van MFA externe apparaten beveiligen en elke inlogpoging verifiëren.

Sociale media

Socialemediaplatforms en -bureaus gebruiken MFA om de persoonsgegevens van miljarden gebruikers wereldwijd te beschermen.Bedrijven zoals Facebook gebruiken een authenticatie om hun ontwikkelaars tegen hackpogingen te beschermen wanneer ze werken op de interne netwerken van het bedrijf.

MFA maakt beveiliging voor socialemediabedrijven ook makkelijker door de toegangsprocedure voor ontwikkelaars te vereenvoudigen. Op cloud gebaseerde MFA oplossingen beschermen ontwikkelaars, en op hun beurt ook gebruikers, doordat het installeren van hardware en software overbodig wordt.

Overheid

De huidige IT-ontwikkelingen stellen overheidsinstanties voor een hele uitdaging om snel veranderingen door te voeren in hun infrastructuur met het oog op de transitie naar de cloud en mobiel.

MFA-technologie helpt overheidsinstanties bij het opstellen van een Zero Trust-beleid om miljoenen gebruikers toegang te bieden.

V&A

Wat als een gebruiker zijn/haar mobiel toestel verloren of vervangen heeft?

MFA berust op gebruikers die over een toestel beschikken waarmee ze zich kunnen identificeren. Als die smartphone of laptop verloren, gestolen of vervangen is, kunnen gebruikers zelf een nieuw toestel registreren door hun wachtwoord opnieuw in te stellen via CSL Live. Als de gebruiker een nieuwe telefoon of laptop koopt kan hij/zij deze functie ook gebruiken om MFA op hun nieuwe toestel te registreren. Waar een gebruiker ook is in de wereld en welke technologie hij/zij ook gebruikt, zijn/haar informatie zal steeds veilig zijn.

Kan ik MFA instellen op meerdere toestellen?

Ja, u kunt MFA instellen op meerdere toestellen – MFA maakt het mogelijk om meerdere

toestellen aan uw account te koppelen.

Mijn gekozen authenticator staat niet in de lijst, kan ik deze gebruiken?

CSL heeft de in dit document genoemde authenticators gestest en goedgekeurd. Wij raden aan dat u deze authenticators gebruikt om de betrouwbaarheid en de toegankelijkheid van uw CSL Live account te garanderen.

Ik kan geen authenticator-app gebruiken, zijn er andere opties?

We hebben alternatieve opties ontwikkeld via SMS en e-mail voor het geval u geen authenticator-app kan gebruiken, om welke reden dan ook. Het volstaat om de optie SMS of e-mail te kiezen wanneer het systeem u vraagt om een eenmalige code in te voeren. Alle SMS/e-mails verlopen na 60 seconden.

Waar vind ik meer informatie terug?

Voor meer informatie over MFA standaard praktijken en -richtlijnen, gelieve op onderstaande links te klikken.

National Cyber Security Centre

National Institute of Standards and Technology