PREVENTIEKAART

MULTI-FACTOR AUTHENTICATIE

Voorjaar 2025

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Multi-Factor Authenticatie (MFA) voegt een extra beveiligingslaag toe aan inlogprocedures. Dit voorkomt ongeautoriseerde toegang, zelfs als wachtwoorden worden gelekt of gestolen.

1 > WAT IS MFA EN WAAROM IS HET BELANGRIJK?

MFA vereist twee of meer verificatiefactoren om toegang te krijgen tot een systeem. Dit verlaagt het risico op phishing, wachtwoordlekken en brute-force aanvallen.

Veelvoorkomende factoren:

- Iets wat je weet (wachtwoord, pincode);
- Iets wat je hebt (authenticator-app, SMS-code, smartcard);
- Iets wat je bent (vingerafdruk, gezichtsherkenning).

2 > IMPLEMENTATIE VAN MFA IN DE ORGANISATIE

Kies voor applicaties die MFA ondersteunen. Op het moment dat je kunt kiezen voor een zelfde soort applicatie mét of zonder MFA, kies dan voor de veiligere, met MFA beveiligde, applicatie.

Stel MFA verplicht voor minimaal alle kritieke systemen en cloudomgevingen. Gebruik een authenticator-app op je smartphone in plaats van SMS/mail voor verhoogde veiligheid. Zorg dat MFA correct is ingesteld op alle apparaten en accounts. Train medewerkers in veilig gebruik en het herkennen van phishing-aanvallen. Zo wordt de kans op cyberaanvallen aanzienlijk verlaagd.

3 > IMPLEMENTATIE VAN MFA VIA MICROSOFT 365

Activeer zelf MFA via Entra (voorheen Azure Active Directory) of vraag uw IT-leverancier.

- Stel MFA verplicht voor alle Microsoft 365-gebruikers, vooral voor beheerdersaccounts;
- Gebruik Microsoft Authenticator als authenticator-app;
- Zorg voor back-up methoden, zoals telefoonnummers of een alternatieve verificatieapp;
- Configureer Entra om extra beveiligingsregels in te stellen.

4 > BEHEER EN ONDERHOUD IN MICROSOFT 365

Controleer en monitor MFA-instellingen via het Entra. Stel meldingen en logging in om ongebruikelijke aanmeldpogingen te detecteren.

Stel een duidelijk beleid in voor het resetten van MFA bij verlies van toegang, bijvoorbeeld na verlies of diefstal van een telefoon.

Overweeg het gebruik van Single Sign-On (SSO). SSO stelt gebruikers in staat om met één set inloggegevens toegang te krijgen tot meerdere applicaties. Dit verbetert de beveiliging door het verminderen van wachtwoordvermoeidheid, het centraliseren van toegangsbeheer en het snel intrekken van toegang bij vertrekkende medewerkers. Combineer dit met MFA voor extra bescherming.

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant