PREVENTIEKAART

MICROSOFT 365

Q3 2026

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Microsoft 365 heeft veel functies om (bedrijfs)gegevens te beschermen, maar niet alle beveiligingsfuncties staan standaard aan. Onderstaande functies zijn in te schakelen met een basisaccount, zonder dat er extra betaalde producten nodig zijn.

1 > SCHAKEL MULTI-FACTOR AUTHENTICATION (MFA) IN

Doe dat zowel voor gebruikers (users) als beheerders (admins) en controleer de werking.

2 > STEL IN AAN WELKE EISEN WACHTWOORDEN MOETEN VOLDOEN

U stelt dat voor alle accounts in via User Password Policies of via Entra-beheercentrum > User.

3 > VOEG HET BEDRIJFSLOGO TOE AAN DE LOGIN PAGINA

Door corporate branding herkennen medewerkers de pagina en vermindert de kans op phishing.

4 > ZET VOOR ADMINS AUTOMATISCH UITLOGGEN AAN

U doet dat via Azure Portal inactivity timeout. U bepaalt zelf het aantal minuten dat de admins inactief kunnen zijn.

5 > VERPLICHT MFA VOOR APPS VAN DERDEN

Blokkeer hiervoor de SharePoint Legacy Authentication.

6 > BEPERK EXTERN DELEN VAN PAGINA'S BINNEN SHAREPOINT

Door External Sharing in SharePoint te limiteren, vermindert de kans dat data (te) lang toegankelijk blijft voor externen of dat de data in verkeerde handen valt.

7 > MAAK EEN EMERGENCY ACCESS ACCOUNT

Zo voorkomt u dat u wordt buitengesloten van uw Azure Active Directory in geval van onvoorziene omstandigheden.

8 > ZET EXTERNAL EMAIL WARNING AAN

Door deze configuratie aan te zetten, informeert u alle medewerkers als een e-mail afkomstig is van buiten de organisatie. Dit verlaagt de kans op succesvolle phishingaanvallen.

9 > GEEF ADMINS ALLEEN DE RECHTEN DIE ZIJ NODIG HEBBEN

Ken Role-Based Access Control toe waarmee ze hun werk kunnen uitvoeren.

10 > CREËER LOGBESTANDEN

Controleer of audit logging in Microsoft Purview is ingeschakeld. Hiermee worden gebruikers- en beheeractiviteiten vastgelegd voor controle, onderzoek en incidentrespons. Let op: de bewaartermijn van auditlogs is afhankelijk van licentie en ingestelde retentie.

i

Er zijn nog meer instellingen mogelijk, maar bovenstaand overzicht heeft prioriteit en maakt uw Microsoft 365-omgeving beslist veiliger. 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