4.3 Wenselijkheid binnen de Werksamen tenant

Een overzicht van verschillende Microsoft Graph permissions, waarbij we aangeven welke permissions ongewenst zijn en we niet toelaten op onze tenant, tot permissions die wij “veilig” genoeg achten en het meest compliant zijn aan de principes van least privileged access en data minimalisatie.

MS Graph permissions matrix van ongewenst naar gewenst				
Ongewenst	>	>	>	Gewenst
5	**4**	**3**	**2**	**1**

Bovenstaand afgebeelde matrix geeft weer welke niveaus van MS graph permissions welke wij hebben vastgesteld van ongewenst (5) naar gewenst (1). Hieronder volgt per categorie uitleg over de permissions en waarom deze in een desbetreffende categorie vallen.

5

Application permissions welke aangemerkt zijn als “gevaarlijk” (*zie ook bronnen onderaan dit document) omdat sommige van deze rechten het mogelijk maken om gebruikers additionele verhoogde rechten aan zich zelf toe te wijzen of geven toegang op het hoogste niveau tot verschillende resources binnen de tenant. Deze rechten (zie onderstaande tabel) zullen **geen** admin

consent krijgen op onze tenant. Deze rechten zijn niet compliant en voldoen niet aan de principes

MS Graph permission	Reden geen Autorisatie
Directory.Read.All	Geeft toegang tot gegevens in alle mappen, ongeacht de gegevensclassificatie. Dit geeft in het bijzonder toegang tot Office 365-groepen met verborgen lidmaatschap.
Groups.Read.All	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap.
GroupMember.Read.All	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap
Groups.ReadWrite.All	Geeft schrijftoegang aan alle groepen.
User.ReadWrite.All	Geeft schrijftoegang voor alle gebruikers
Member.Read.Hidden	Geeft toegang tot Office 365-groepen met verborgen lidmaatschap.
Files.Read.All	Hiermee wordt leestoegang verleend tot alle SharePoint Online en OneDrive for Business bestanden.
Update_device_attributes	Intune bij de gemeente Emmen is ingeperkt en deze permissie geeft de mogelijkheid om elk apparaat dat Intune beheert bij te werken.
Update_device_health	Intune bij de gemeente Emmen is ingeperkt en deze permissie geeft de mogelijkheid om elk apparaat dat Intune beheert bij te werken.
ActivityFeed.Read	Geeft brede toegang tot alle Teams-kanalen.
AppRoleAssignment.ReadWrite.All	Met deze applicatierol kan de gebruiker of applicatie extra privileges toekennen aan zichzelf en aan andere applicaties.
RoleManagement.ReadWrite.Directory	Deze applicatierol bevat ook het recht om admin rechten toe te kennen. Hiermee wordt het mogelijk gemaakt om andere applicatierollen met verhoogde rechten toe te wijzen.

van least privileged access en data-minimalisatie.

4

Rechten die gegevens m.b.t. de identiteit van gebruikers beschikbaar maken voor een derden app. Er zijn 6 admin rechten die afhankelijk van de permissie alle gegevens inzichtelijk maken en niet zijn af te schermen. Daarnaast zijn er 3 rechten vanuit een gebruikersperspectief (Delegated) die mogelijk ook teveel gegevens beschikbaar kunnen maken (echter beperkt zich dit alleen tot waar de gebruiker ook daadwerkelijk toegang tot heeft)

Als onderstaande application permissions benodigd zijn omwille van functionaliteit, dan moet dit worden gedocumenteerd in het ABD (Applicatie Beheer Document). Daarnaast moet er toestemming zijn vanuit de andere gebruikers (klanten en gemeenten) van de tenant, dat hun gegevens inzichtelijk/toegankelijk zijn door derden. Ook moet altijd worden onderzocht of de gevraagde permissies wel daadwerkelijk noodzakelijk zijn en dat minder uitgebreide permissies wellicht ook volstaan.

MS Graph permission	Toelichting
Member.Read.Hidden MSGraph: User.Read.All MSGraph: Group.Read.All MSGraph: Group.Write.All MSGraph: Directory.ReadWrite.All MSGraph: Directory.Read.All	Application permissions waarmee identiteitsinformatie over onze Entra ID tenant kan worden opgevraagd.
MSGraph: User.Read MSGraph: User.ReadBasic.All MSGraph: Directory.AccessAsUser.All	Gebruikersrechten waarmee identiteitsinformatie over onze Entra ID tenant kan worden opgevraagd.*

*Hoewel deze rechten wellicht meer informatie kan blootgeven dan noodzakelijk, worden deze gedaan vanuit een gebruikersperspectief en geeft alleen gegevens over de ingelogde gebruiker waaronder deze permissions worden uitgevoerd.

3

Rechten waar we een admin consent voor afgeven maar alleen onder specifieke omstandigheden. Deze rechten zijn middels een policy in te perken of via aanvullende rechten.

API & Permission Scope	Toelichting
MSGraph: Mail.Read MSGraph: Mail.ReadBasic MSGraph: Mail.ReadBasic.All	Ongepaste lees- en/of schrijftoegang rechten, waarmee toegang wordt verleend tot de mailboxen van alle gebruikers. Gebruik de volgende instructies om deze rechten voor specifieke

MSGraph: Mail.ReadWrite.All MSGraph: Mail.Send MSGraph: MailboxSettings.Read MSGraph: MailboxSettings.ReadWrite MSGraph: Calendars.Read MSGraph: Calendars.ReadWrite MSGraph: Contacts.Read MSGraph: Contacts.ReadWrite Office 365 Exchange Online: full_access_as_app	groepen/gebruikers te beveiligen: Limiting application permissions to specific Exchange Online mailboxes - Microsoft Graph | Microsoft Learn
MSGraph: Sites.FullControl.All MSGraph: Sites.Manage.All MSGraph: Sites.Read.All MSGraph: Sites.ReadWrite.All	Ongepaste lees- en/of schrijftoegang rechten waarmee toegang wordt verleend aan alle Sharepoint Online sites. Gebruik: Controlling app access on a specific SharePoint site collections is now available in Microsoft Graph - Microsoft 365 Developer Blog

2

Wanneer gebruikerssynchronisatie tussen de tenant en derde partij wenselijk is, geven wij de voorkeur voor het inrichten van een runbook (het maken van een geautomatiseerde oplossing) in Azure. Daarbij stellen we als eis dat de gebruikerssynchronisatie wordt gedaan op een Entra ID groep of gesyncte AD-groep waarin de gebruikers lid van zijn die ten behoeve van de app gesynct moeten worden. Daarnaast moet de beveiliging voldoen aan de meest recente (beveiligings-)standaarden van Microsoft.

1

De voorkeur qua rechten gaat uit naar Delegated permissions. Deze rechten worden uitgevoerd uit naam van de gebruiker en de voor hem of haar geldende rechtenstructuur. En voldoet het meest aan de principes van least privileged access en data-minimalisatie.

*bronnen m.b.t. riskante en gevaarlijke application permissions met uitleg en toelichting
Privilege escalation using Azure App Registration and Microsoft Graph · Pim Widdershoven
Entra ID OAuth Admin Consent and Risky Permissions – IT Connect (uw.edu)