Wednesday Offensive

12/17/2025

Sean Metcalf

@PyroTek3

2025: AD Common Security Issues

Group Policy permissions

Modify a GPO to own everything that applies it

AD Permissions

Delegation a decade ago is still in place, so are the groups

Improper group nesting

Group inception = innocuous groups with super powers

Over-privileged accounts

Regular users are admins

Service account access

Domain Admins (of course!)

Kerberos Delegation

Who really knows what this means?

Password Vaults

Management issues (user accounts with admin rights, improper protection of server, etc)

Backup Process

What servers backup Active Directory? How is this backup data protected?

Entra ID Common Security Issues

Privileged Account Issues

- Standard user accounts are members
- Service Accounts / Service Principals are members
- Account(s) authenticate from user workstations
- Using PIM, but all/most are permanently active, not eligible.
- MFA not configured on highly privileged role members

Applications with Highly Privileged Permissions

- Highly privileged applications (Trimarc Level 0) with standard user account as owner
- Standard user account in Application Administrator and/or Cloud Application Administration role(s).

Group Nesting

- Role Assignable Groups in highly privileged roles (Trimarc Level 0)

Partner Access - Delegated Access Permissions

- Global Administrator
- Helpdesk Administrator

TrustedSec Tier 0 Applications

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

Directory.ReadWrite.All

- “Directory.ReadWrite.All grants access that is broadly equivalent to a global tenant admin.” *

AppRoleAssignment.ReadWrite.All

- Allows the app to manage permission grants for application permissions to any API & application assignments for any app, on behalf of the signed-in user. **This also allows an application to grant additional privileges to itself, other applications, or any user.**

RoleManagement.ReadWrite.Directory

- Allows the app to read & manage the role-based access control (RBAC) settings for the tenant, without a signed-in user. This includes instantiating directory roles & **managing directory role membership**, and reading directory role templates, directory roles and memberships.

Application.ReadWrite.All

- Allows the calling app to create, & manage (read, update, update application secrets and delete) applications & service principals without a signed-in user. This also allows an application to act as other entities & use the privileges they were granted.

Level 0 Entra ID Roles (First 5 to focus on)

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

- **Global Administrator**
  - Full admin rights to the Entra ID, Microsoft 365, and 1-click full control of all Azure subscriptions
    From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path (2020)
- **Hybrid Identity Administrator**
  - *"Can create, manage and deploy provisioning configuration setup from Active Directory to Microsoft Entra ID using Cloud Provisioning as well as manage Microsoft Entra Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single Sign-On (Seamless SSO), and **federation settings**."*
    https://medium.com/tenable-techblog/roles-allowing-to-abuse-entra-id-federation-for-persistence-and-privilege-escalation-df9ca6e58360
- **Partner Tier2 Support**
  - *"The Partner Tier2 Support role can reset passwords and invalidate refresh tokens for all non-administrators and administrators (including Global Administrators). "*

    "not quite as powerful as Global Admin, but the role does allow a principal with the role to promote themselves or any other principal to Global Admin."
    The Most Dangerous Entra Role You've (Probably) Never Heard Of
- **Privileged Authentication Administrator**
  - *Microsoft: "do not use."*
    "Set or reset any authentication method (including passwords) for any user, including Global Administrators. …
    Force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke remember MFA on the device, prompting for MFA on the next sign-in of all users."
- **Privileged Role Administrator**
  - *"Users with this role can manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management. …*
    This role grants the ability to manage assignments for all Microsoft Entra roles including the Global Administrator role. "

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Stay Up to Date on Entra ID Security

Sean’s Entra ID Security List:
PyroTek.io/EntraIDSecurityList

References

- Merril’s Conditional Access Documenter https://idpowertoys.merill.net/ca
- TrustedSec Post on Entra ID Privileged Roles https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach
- Brandon’s post on Emergency (Break-Glass) Admin Accounts https://practical365.com/lifeline-or-liability-managing-emergency-accounts-in-hybrid-environments/
- Improve Entra ID Security More Quickly https://adsecurity.org/?p=4825
- Active Directory Security Tips https://adsecurity.org/?tag=activedirectorysecuritytip