Tier 0 A/DA/EA Groups

How often do you ask the question, “How many Domain Admins do we have?” Probably more often than you ask, “Who is in the group policy creator owners group today?” Active directory creates a number of groups with every new domain deployment. They are often the building blocks of privileged access in a domain.

These groups have inherited permissions, often overlooked in environments. By default most of the groups listed in this series are empty. As companies grow and administration of the identity system changes hands, groups tend to accumulate users.

Builtin Groups-1

The results of Gap Analyses that I’ve completed often show these groups with 100+ users added directly to them. This high number I’d a far cry from the default zero. In the worst examples, every single user in a domain is added to a privileged group often by accident.

For a full list of permissions on the default built in groups, please reference the Microsoft article:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b–privileged-accounts-and-groups-in-active-directory

Now to dive right into sensitive rights a select few of these groups have…

The list of groups covered in this series, in alphabetical order: Account operators Administrators - covered in this post Backup operators Domain Admins - covered in this post Enterprise admins - covered in this post Exchange groups - quick list Group policy creator owners Print Operators Remote desktop users Server operators

Each group will be defined with

My everyday and very general definition. Security fears related to the rights granted to the group. Basic recommendations to perform on the group listed

Administrators Defined:

Often overlooked by auditors, this group is God-Mode. Full access to all objects on the domain.

Danger:

Groups or users are often added directly to this group Default audits only require reporting on “Domain Admins” and pften overlook this group Recommendation:

Audit the group membership, starting today Remove any groups nested inside this group besides: Domain Administrators and Enterprise Administrators Remove any users added directly to this group

Domain Admins Defined: This group is nested in the administrators group (nested god mode). By default it is also listed as administrator on all workstations and servers in the domain.

Danger:

Everything from the administrator list Member of every computer's admin group Recommendation:

Limit this group to 5 users max Admins: Get in a room to talk about who needs to be in this group. Look around the room. Identify everyone in the room at that moment. Kick everyone out of the group that is not currently in the room Audit login event for all domain admin account activity

Enterprise Admins Defined: Forest administrators. The EA group is granted rights to affect forest wide changes: adding/removing domains, creating trusts, upgrading/raising forest levels

Danger:

This group isn't often needed after the initial setup of a simple domain Can create rogue trust to compromised domain. This would provide a direct persistent path to compromise a domain Recommendation:

Remove all users and groups from this group Monitor group's additions and removals

The above groups should be the groups auditors are checking. If you are planning on creating a self directed risk assessment begin your documentation with a confirmation that these groups are on your audit list.

These groups listed are the first groups that attackers are attempting to compromise. If attackers are able to quickly and efficiently compromise these groups, they have an immediate return on investment. The attacker wins. You must begin a security plan by securing these groups.