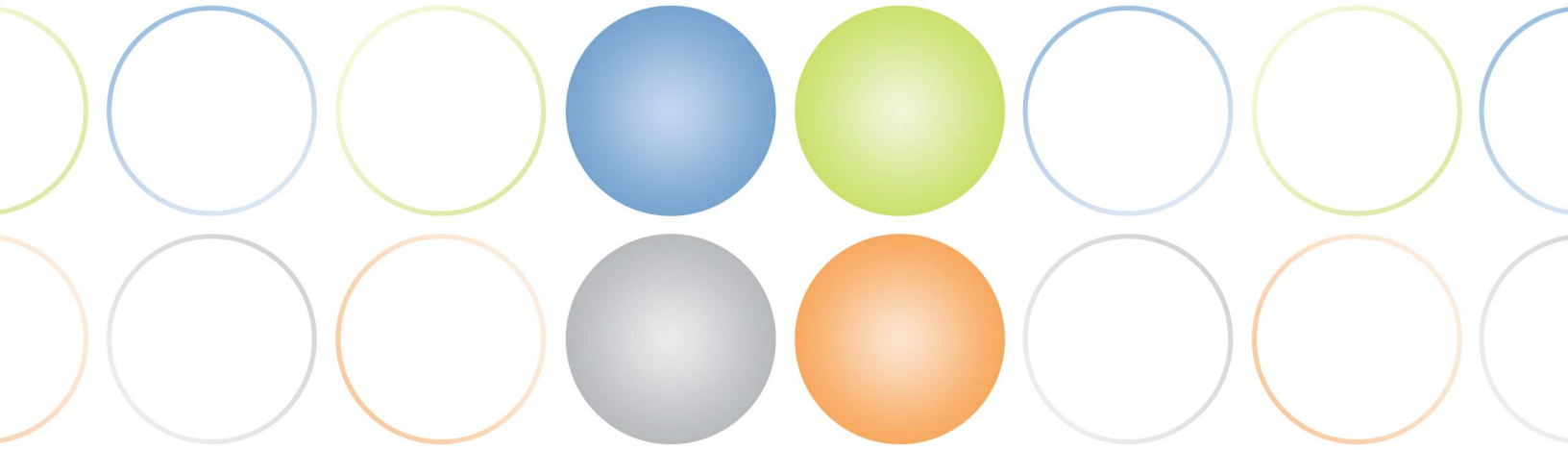
WHITEPAPER

Insider Threats, Least Privilege, and the Risk in AD Groups



Every IT organization is working tirelessly to reduce threats that may pose a risk to their data, applications, and systems. With so many potential attack vectors, the question of where you will see the greatest security return on your protection effort investment is both warranted, and critical to the success of your security initiatives. The good news is that the answers are well-founded in reputable industry data.

Approximately **30%** of all data breaches involve insiders . And, while external attacks represent the bulk of data breaches – coming in at just under **70%** of attacks[1], the #1 threat action by external attackers is the use of stolen credentials[1]. In essence, even an external attack eventually looks like an insider attack. So, if you're trying to decide where to place your security efforts, thwarting insider threats should definitely be at the top of the list.

One of the largest challenges with insider threats is that they involve the misuse of privileges already assigned to the individual - usually in order to accomplish their assigned work tasks. Because of this, it becomes difficult to tell whether an action performed by an insider is appropriate or not – so difficult, that ***82%*** of insider data breaches take months or years to be discovered[1].

So, how do you address insider threats?

There are three basic components to an insider threat strategy – the first is reducing the risk and impact of an insider threat, the second is detecting potential threat activity, and the third is responding to those activities appropriately. In this paper, we'll focus on a major source of insider threat risk and the steps you can take to limit the exposure and impact of insider threat activity.

Mitigating the Threat of Insiders

To mitigate risk, it's critical to begin a conversation around the concept of least privilege – ensuring users have only the permissions needed– especially in scenarios where an external attacker has compromised a set of credentials. What makes this so important is the fact that users today, in many cases, actually have far more permissions than needed by the user and intended by IT.

In a recent Ponemon study[2] , 71% of end users stated they frequently or very frequently have access to information they shouldn't. And with permissions granted in Active Directory serving as the basis for all permissions on-prem, in Office 365, and any AD-integrated cloud applications, this over-permissioning of user only exacerbates the insider threat problem, providing access to the insider well beyond the corporate walls and into the cloud.

Then, what's the source of over-permissioning? Simple – it's ***IT***.

[1] *Verizon, Data Breach Investigations Report (2017)*

[2] *Ponemon, Corporate Data: A Protected Asset or a Ticking Time Bomb? (2014)*

Without proper controlling of permissions – found in the day-to-day management of Active Directory groups – IT itself is actually contributing to the potential of a threat event. Think about it – if nearly three-fourths of your users have too many permissions, it's because IT isn't doing the work of cleaning up groups and the permissions assigned to them on a continual basis.

There are plenty of sources from which group dis-organization evolves. When users change positions, they get added to groups associated with their new role. Over time, these groups become outdated and repurposed (based on, then, current membership) and given a new life with newly assigned permissions. In some cases, permission assignments are made to a group without first-hand knowledge of how a group is used. And, in none of these familiar examples do you see IT cleaning up the old permissions, or memberships, as users rarely ask that their access (via group membership) be removed, as it is no longer relevant to their ever changing responsibilities or roles in the organization. It's an unfortunate truth, but one that all too often exists.

So, what can IT do to reduce the risk of insider threats?

While you can't entirely stop an insider from stealing corporate data, you can shrink the threat potential by ensuring users only have the needed permissions and nothing more. To do this, IT organizations need to follow 3 simple steps:

- ***Assess:*** Understanding the current state of (in)security
- ***Assign:*** Bringing groups into a secure state
- ***Administrate:*** Establish group lifecycle management policy and process

Let's look at each to see the work necessary to reduce insider threats.

Step 1: Assess: Understanding the current state of (in)security

You cannot improve security without first gaining a full understanding of just how secure – or insecure – your environment is. Insiders (and external attackers with compromised credentials) will leverage every and all permissions they have at their disposal. To minimize the risk, the goal here is to identify how users are gaining access to resources via AD groups, and to determine whether that access is appropriate. This involves a few tasks:

- ***Get Close to the Group -*** If you have hundreds or thousands of groups, it's very likely IT has zero idea what the purpose of each group is anymore. So, it's important to obtain insight and context from someone within the organization who is close to the actual use of the group and the access its membership grants. This can be an application owner, a line of business manager, or a department head. Ask about the access necessary, users that need such access, and whether either of those change over time. FYI, you'll be utilizing this person again in a later step.
- ***Assess Group Permissions -*** Review the permissions assigned to a group using resource-specific management tools.

- ***Assess Group Membership*** **-** Build out a list of users that are group members and, if possible, determine how long each user has been a member.

- ***Assess Group Nesting*** **-** Don't forget some permissions may be obtained through nesting, so repeating the process of assessing the group membership for each nested group (and even multiple layers of groups nested within groups) is needed.

If you were to stop here, you've likely come to the conclusion this could prove to be quite a bit of work. So, focus on groups that provide access to critical resources first. You're looking for misalignment between the needs of the business (provided by the person you utilized to provide usage details of a given group) and the actual execution of security (as exemplified by the group details found during the assessment).

You also may find groups that have no members, repurposed groups, groups with stagnant memberships, or groups with constantly changing memberships. These should be noted and investigated, as each of these scenarios can indicate long-term mismanagement of a given group – which may constitute a potential threat risk.

Once the assessment is complete, you now have a clear idea of what needs to be fixed.

Step 2: Assign: Bringing groups into a secure state

Whether you've chosen to perform an assessment of all your groups before making any changes, or you are working through all of the steps in this paper one group at a time, the next step is to rectify any issues found. Like applying patches to systems and applications, each assignment fixes a gap found in the assessment. Tasks should include:

- ***Update Group Details*** – this is the perfect time to determine whether the groups have a purpose-driven name and/or description documented to ensure proper usage and membership of a given group.

- ***Modify Group Membership*** – In the simplest of cases, you'll need to ensure only necessary users and groups are members of groups.

- ***Create New Groups*** – Your assessment may uncover that groups have been repurposed, having new permissions assigned to additional resources, but without cleaning up the membership and old permissions that do not reflect the group's current use. So, it may be necessary to create new groups to ensure only the current mix of users and access exists. This task may also be part of a process to split out an older usage of a group (complete with its own old permissions and members) from its current use.

- ***Recreating Groups*** – IIn cases where you cannot validate all permissions assigned to a group, it may be necessary to recreate security by recreating the group, assigning proper permissions and memberships, and removing the old group.

- ***Delete Old Groups*** – In many organizations, groups live forever. So, it's possible to find a group that exists having membership and access that is no longer needed by the business. Since we all know IT never deletes groups in AD, this step will be necessary – as difficult as it may be for some of you. Third-party solutions can also archive a group, to allow for it to be recovered at a later date.

If you've completed the first two steps for all of your groups, you'll be in a position where today your groups, membership, and access are in a known, secure state.

But, what about a week, month, or year from now?

Because you don't have the time to stop what you're doing and perform such a monumental project periodically, what needs to be done is to put in place a means by which groups, their membership, and the assigned permissions can remain both known, and consistent with IT's intent.

Step 3: Establish group lifecycle management policy and process

All of the cleanup accomplished via the first two steps represents some of the work that should go into a group's lifecycle: every group should be properly configured to meet the current needs of the business – keeping in mind, those needs change over time. But to keep group management from backing up (like it has before, causing you to go through steps 1 and 2 to get things cleaned up), look to put policy and process in place that control each group's configuration over time. This should include:

- ***Group Ownership*** – That person you used to assess a group's use should be assigned as the group's owner. This means they should be responsible to manage the group through its lifecycle, including management in AD (yes, a user outside of AD who actually knows how the group should be used is a better choice than some low level IT person who has no idea whether Dave should be added or not), approve any membership or access changes, and, eventually, requesting deletion of the group. Native tools only allow a single account, but keep in mind Group Lifecycle Management best practice dictates having multiple owners in some circumstances. Third-party solutions may be needed to accomplish this.

- ***Group Changes*** – Processes need to be put in place where anytime any changes to a group's configuration, membership, or permissions assigned are to be made, the group owner must approve the change. This ensures the owner is completely aware of the current state of a group.

- ***Group Self-Service*** – If groups are named properly, and with the right tools in place, it's feasible for users to request membership to groups to accomplish tasks. This takes the burden off of IT and places it on the group owner to approve. a group.

- ***Group Attestation*** – Periodically, IT and group owners need to meet to attest to the memberships, permissions, and the very need for each group. This process keeps IT informed, maintaining least privilege to reduce the impact of any insider threats.

By performing these tasks, you continually put groups – and, therefore, the organization – in a constant, and current, state of security, eliminating an insider's ability to misuse inappropriate access that simply shouldn't exist.

Minimizing Insider Threats with AD Groups

Insider threats may be a true insider – an employee leveraging the access their job affords – or can be an attacker misusing compromised credentials, looking for any kind of access the credential has. As part of an insider threat prevention and response strategy, one of the first steps organizations need to take is to limit your organization's exposure by implementing least privilege.

By assessing and cleaning up your current AD groups, user access will be limited, thereby reducing the exposure during an insider threat scenario. Implementing group management lifecycle processes puts your organization in continual control over the state of exposure, leveraging those closest to a group's usage – the users themselves – to keep the configuration of your security via AD groups up-to-date.

About Imanami

Founded in 2001, Imanami Corporation is dedicated to helping businesses across the globe maintain the health of their Microsoft® Active Directory groups. Imanami's flagship product is GroupID, a suite of powerful group management tools.

For many IT professionals, managing AD groups can be an overwhelming challenge: Employees move locations, change departments, and start new groups all the time. As a result, IT professionals are faced with the daunting task of continually managing and updating security and distribution groups — often having to do so manually.

GroupID from Imanami makes it easy to stay on top of all the changes, requests, and requirements that IT sees every day.

To learn how GroupID might be able to help, please visit ***imanami.com.***