SECURITY BOULEVARD

Cleaning up the Active Directory Forest

September 3, 2020

Used by many organizations and enterprises, Microsoft's Active Directory (AD) comprises several services that run on Windows Server to manage permissions and access to networked resources. Within the Active Directory configuration hierarchy, an AD Forest is the most important logical container. Chances are you've inherited your AD Forest from a former systems administrator. In fact, the average AD Forest is typically around 14 years old. Depending on your organization's history, you may have no idea what policies were in place before you took on your role or how they were enforced.

Ninety percent of the world's enterprises rely on Active Directory as their primary mode for authentication and authorization, making it crucial to have awareness of any and all potential security holes across corporate AD environments. Rather than dig for fossils in your AD Forest and trying to understand the history of its infrastructure, there are ways to easily identify and patch vulnerable areas and ensure a strong security posture. Here's a guide to identifying the top four most common AD Forest vulnerabilities and how to mitigate them.

Vulnerability 1: 'Password' Is Not a Password

Many organizations are guilty of allowing years-old service accounts to keep the same passwords from their original creation, many set to never expire. The problem here isn't so much that passwords need to be changed regularly—in fact, NIST guidelines now recommend changing passwords only after experiencing a threat that could compromise the account's security.

However, picking an easy password such as "abc123" or "password" is not sufficient. The NIST guidelines recommend that passwords are at least eight characters long, or six characters chosen randomly.

Additionally, users should be careful not to reuse passwords for multiple accounts. Too frequently, users have the same passwords for professional and personal accounts, for email and social network accounts.

The Solve: This is a fairly simple problem to fix with ongoing organizational education. Help employees understand how to create strong passwords, why they should create separate passwords for individual accounts, and how to spot potential phishing attacks. On an organizational level, make sure accounts are regularly monitored for suspicious activity and enable multi-factor authentication.

Vulnerability 2: Reassess Your User Governance Policies

Longtime employees frequently get added to a number of groups throughout their tenure. For example, if an employee starts off in HR, but then moves into a sales or marketing role, they will often accumulate groups that align with each role or title. There's also the issue of users having delegated rights for past situations no longer relevant today, leaving them with permissions they don't need or shouldn't have. Ideally, employees should be removed from groups and rights after they switch roles or no longer require them. Additionally, permission settings are infrequently reassessed, which means they're outdated and irrelevant to current security policies.

When employees are members of multiple groups within an organization and have delegated rights not relevant to their work, it increases the attack surface and makes it easier for bad actors to gain access to privileged information.

The Solve: Organizations will need to review employee permissions and remove those that are no longer appropriate to mitigate security issues before they arise. Multiple levels of management need to have awareness of this project for it to be executed completely. With a combined, shared understanding of administration tasks, teams can develop an automated policy that removes outdated permissions and prevents "permission creep."

Vulnerability 3: Removing Built-In Privileges

Frequently, standard user accounts will be given privileges to sensitive administrative groups. If a standard user has access to privileged groups within the environment, attackers can easily gain access to the AD database by using brute force to discover passwords. Organizations should create policies that contain no day-to-day users by default and only add users when needed for specific build and disaster recovery situations.

The Solve: Teams must move away from manual knowledge-sharing administrative techniques. The first step to solve this is to remove empty groups. This may be a scary step, given fears that a group may be needed, but once it's determined if a group has any rights within the environment then you can easily skip over groups that are not in use.

Next, create a policy for group creation. This will ensure that groups follow a naming convention and that each group has an owner and follows a specific workflow for regular approvals. These should also set to expire after project completion so that your AD only contains active groups.

Last, review the membership of sensitive groups such as Enterprise Admins, Domain Admins and Account Operators. These groups should only contain essential accounts and the remaining accounts should be audited regularly.

Vulnerability 4: Update Your Operating Systems

You may not need to change your password as frequently as you thought, but you will need to change your operating systems. Too often, users are running operating systems that have passed their end of support date, making them primary targets for hackers as newly discovered security patches won't be patched.

Even supported operating systems could be vulnerable to attacks if they are not regularly assessed for security patch updates. For example, in 2019, researchers uncovered BlueKeep, a vulnerability in Windows 7 and Windows XP—which were still supported by Microsoft at the time—that allowed attackers to remotely connect to Windows servers and spread malware rapidly between devices.

The Solve: Remove all unsupported operating systems and migrate all apps, platforms and data to a supported and secure operating system. Also, ensure there's a policy in place for all desktops, laptops and servers to capture all security updates as they're released.

Trimming the AD Forest Underbrush

Inheriting your organization's Active Directory Forest with little to no context on previous policies can be a challenge, but the key is to take the process one a step at a time. Identify potential vulnerabilities, mitigate the current threats and work with the broader organization to ensure there are policies and tools in place to ensure these issues are patched and protected from attackers.

Source: https://securityboulevard.com/2020/09/cleaning-up-the-active-directory-forest/