CyberFOX™

UNDERSTANDING LEAST PRIVILEGES

INTRODUCTION

As an IT professional, you're aware of the importance of defense-in- depth when it comes to protecting yourself and your users; IT professionals must use layered security to protect the data and assets under their custody. That said, many in the IT world overlook a simple but critical step in curtailing cyber-attacks early in their lifecycle by failing to restrict local administrator rights.

User accounts with local admin rights possess virtually unlimited access to do anything they want on their device(s). When a user has admin access, they can download and install applications, use any program, change system configurations, and even modify or revoke other administrative accounts. Such power nullifies much of the protection offered by perimeter cyber defense.

A user with local admin rights can easily bypass or remove measures like firewall and antivirus and install malware, steal data, or conduct other malicious actions. In short, admin privilege gives a user --or a compromised user --the metaphorical "keys to the castle".

WHAT ARE PRIVILEGES AND HOW ARE THEY CREATED?

When speaking of information security, privilege is often defined as the authority a given account or process has within an IT environment. Local admin privilege on a workstation endows the user with the power to disable or bypass many security restraints. Such a user will have permissions to perform such actions as shutting down systems, installing drivers, configuring hardware, provisioning other accounts, and disabling security protocols.

Privileges are critical to IT operations and serve an important purpose when used correctly. The ability to create privileges allows IT professionals to assign users, applications, and other system processes various levels of rights to access resources.

The ability to denote privileges for user accounts and operational processes is built into operating systems, file systems, databases, hypervisors, cloud management platforms, and many enterprise software applications. Global or granular privileges can also be configured by system or network administrator in other instances.

Depending on the IT landscape, some privilege assignments may be based on attributes that are role-based. For instance, members of different departments may have different levels of access because their accounts are assigned to different role groups. These decisions are typically based on what level of access is needed to complete their normal tasks.

What is a Privileged Account?

A privileged account is considered to be any account within this system of roles or groups that provides access beyond those of non-privileged or "standard" accounts. Any user with privileged access, typically gained by ownership of a privileged account, is known as a privileged user.

There are also unique privileged accounts called "superuser accounts" which are typically used only by IT administrators. These accounts provide virtually unrestrained access and abilities within the system. These superuser accounts are known as "Root" accounts in Unix/Linux and "Administrator" accounts in MS Windows systems.

Overview of Common Account Types

Local administrative accounts- Accounts providing administrative access to the local host or instance.

Domain administrative accounts- Accounts granting privileged administrative access across all workstations and servers within a certain domain.

Break-glass or emergency accounts- Accounts with administrative access to secure or recover systems, sometimes made available to normally unprivileged users for emergencies.

Service accounts- Privileged accounts used by an application or service to interface with the operating system.

Active Directory or domain service accounts- Accounts primarily in place to make changes to other accounts or groups.

Application accounts- Accounts used by software applications to access databases, run scripts, or provide access to other applications in the course of operation.

WHAT IS THE PRINCIPLE OF LEAST PRIVILEGE?

Because of the power available to admin users, cybersecurity experts recommend that all IT professionals adhere to the principle of least privilege. It's been found that 80% of security breaches involve compromised privilege credentials. The principle of least privilege applies in a wide variety of settings, but we're primarily focused on how it applies to networks, systems, and data.

This principle --also known as "least privilege access" --is the idea that users in the IT environment should only have access to what they need in order to perform their responsibilities, and nothing more. This maxim arises from the fact that the more resources a user has access to, the greater the potential danger if their account is compromised or if they become an insider threat.

For example, a member of the organization may need access to the company website hosted on company servers because they're part of the web design team. While it's true they need access to the site's file system, they do not need the ability to configure the server or to access other data stored within. Any access they have beyond what is needed to complete their job puts additional resources at risk.

Least Privilege and Zero Trust

“Zero Trust” is a security philosophy that assumes any user or device is a potential threat. Whereas older security philosophies believed that any activity originating from within the network was trustworthy, Zero Trust recognizes that vulnerable endpoints, social engineering, and insider threats pose a great deal of risk.

The principle of least privilege is an important part of Zero Trust security. A Zero Trust network gives users and devices only the access they absolutely need and takes a granular approach to access management. Without limiting user privileges there can be no true adherence to the principle of Zero Trust.

> *“Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.”*
>
> **US National Security Institute**

WHY LEAST PRIVILEGE IS IMPORTANT

The dangers of unrestricted admin user accounts should be clear by now. Studies show that 56% of security breaches take months or longer to discover. If a malicious actor compromises a user account with local admin privileges, the impact is quite far reaching.

Once a hacker has gained privileged access, they are free to take a number of escalating actions

- They can disable perimeter security measures and endpoint security such as antivirus
- They're free to install malicious software and proliferate it throughout the network
- Encrypting data with ransomware becomes trivial and can be done in seconds
- The bad actor can move freely within a network
- They can turn any of the organization's systems against them

BENEFITS OF REMOVING LOCAL ADMIN RIGHTS

While users enjoy the freedom of having local administrative rights on their workstations, this is a convenience that comes at a price.
When users can add or remove programs, install devices, and configure security tools without approval from the IT department, a great deal of risk is created.

Removing local admin access sometimes frustrates users who are used to complete freedom without having to ask for permissions from IT. In smaller organizations, this can even be viewed as an inconvenience to the IT team itself.

However, there's no longer a margin for error and convenience is no longer an excuse for ignoring admin privilege management.

The benefits of privileged access management include

- A reduced risk of malware infections
- Secures antivirus and other protections from outside intervention
- Eliminates an attacker's ability to exploit the majority of known vulnerabilities

As you know, most of your users do not need local admin access to perform their jobs. Even company leadership rarely needs that level of access. However, some cases will always require higher privileges. Tools like AutoElevate help to manage these situations by sending the IT team notifications when access is requested. The IT professional can then quickly evaluate and then approve or deny the request right from their smartphone or workstation.

WHAT IS PRIVILEGED ACCESS MANAGEMENT?

Privileged access management (PAM) is a subset of cybersecurity that revolves around tools and methods for controlling the access and permissions for users, accounts, processes, and systems throughout an IT environment. Because it is a process-based approach to all of the concepts we've discussed above, PAM helps IT departments and end users reduce their organization's attack surface and prevent or minimize the damage arising from intrusion.

Privileged account management is sometimes referred to as privileged identity management (PIM), or just access management. PAM is considered by many IT experts and cybersecurity leaders as one of the most important security projects for reducing cyber risk in the modern threat landscape. Of course, the central strategy behind PAM is the restriction of access rights and permissions for users, accounts, systems, software, devices, and computing processes according to the principle of least privilege.

Privilege management is thought of as a subdomain of identity access management (IAM). Both PAM and IAM work together to provide control, visibility, and accountability over all credentials and privileges with the IT environment.

CONCLUSION

Now that we've reviewed the nature and importance of privileged access management, you're probably wondering how to most efficiently and easily conduct PAM across an entire list of clients? While this could be a daunting challenge, AutoElevate is a PAM tool which makes securing your users easier than ever.

Considering moving your users to a Least Privilege security model?

AutoElevate provides

- Remove local admin privileges –without frustrating users
- Least privilege 'baked-in'
- Audit & remediation
- Fully customize windows privileges
- Meet security & compliance goals in minutes
- Not Active Directory dependent
- Malware protection

AutoElevate by CyberFOX

Privileged Access Management for MSPs and IT Pros

Lock everyone down on Standard privileges without frustrating end users. Protect your company from ransomware attacks with the simplest privilege management solution.

With AutoElevate IT departments get

- Malware protection
- Least privilege 'baked-in'
- Audit & remediation
- Remove local admin privileges – without frustrating users
- Fully customize Windows privileges