Windows IT Pro

The Importance of Managing Privileged Accounts

By Orin Thomas

MCITP, MCSE, MCT, Microsoft Consumer Security MVP

Contents

The Importance of Managing Privileged Accounts

By Orin Thomas
MCITP, MCSE, MCT, Microsoft Consumer Security MVP

Best practice for the use and management of privileged accounts is a topic that even experienced IT professionals find complicated. Rather than explain the complexities of privileged accounts to non-technical organizational leadership, IT professionals unintentionally let management assume that everyone in the IT team has "the keys to the castle."

While it is possible to us a nuanced privilege strategy to manage an organization's information systems, pursuing such a strategy often seems too complex and time consuming. IT professionals need to ensure that important maintenance and management tasks can be completed in a timely manner, so they often take steps like sharing the passwords for very powerful accounts so that anyone on the IT team can perform these tasks. However, the IT professional's need to perform tasks quickly and efficiently must be balanced against management's need to ensure that administrative privileges are used in a way that is accountable. If everyone has access to "the keys to the castle," it can be difficult to figure out who left the drawbridge down.

Moreover, proper management and accountability for the use of privileged accounts is not just a matter of bringing peace of mind to organizational leadership; it is also becoming a compliance obligation. Governments are passing legislation detailing the steps organizations must take to manage privileged accounts, just as they have passed legislation detailing competition policy and acceptable accounting practice. Therefore, taking a hands-off approach and allowing the IT department to police itself when it comes to the management of privileged accounts not only presents a security risk, but might also invite sanction from regulatory authorities.

Understanding Administrator Accounts and Privileges

What Rights Do Privileged Accounts Have?

Understanding what you can use privileged accounts to accomplish is not as straightforward as it might seem. This is because privileged accounts come in a variety of shapes

and forms. Put another way, not all administrator accounts are equal. At a basic level, a privileged account is an account that can be used to perform tasks that an ordinary user account cannot perform. Some privileged accounts almost have access to everything on the network. Other administrator accounts might be able to perform only basic tasks, like backing up a database.

How accounts get these rights varies from system to system, and from application to application. Some products allow only a single all-powerful Administrator account, which forces teams of IT professionals to use and share a single set of credentials, irrespective of their actual duties in managing the product. Other products allow a more nuanced approach, allowing IT professionals to use separate accounts to perform different administrative tasks. There are almost as many ways of assigning rights to accounts as there are different products. Although there is a move toward role-based access control (RBAC) as a best practice, use of RBAC is still the exception rather than the rule. Unless a consistent and methodical approach to privilege assignment has been taken from the outset, it can be challenging to determine precisely what privileges a specific account has been assigned.

How IT Professionals Use (and Misuse) Privileged Accounts

In many cases, as a way of simplifying the complexity of privilege management, IT professionals choose to use a single all-powerful account and to then share the credentials for that account across the team. While this certainly ensures that IT professionals can get their jobs done, it raises issues in terms of accountability and organizational security.

In fact, it's an open secret that some IT professionals have questionable habits when it comes to the use of their own administrative credentials. These habits tend to develop not because IT professionals are negligent, but as a practical way of reducing the complexity of their job. For example, the following behavior is common unless some sort of privileged account management strategy exists:

- Highly privileged accounts are often shared between IT professionals. This happens because some products and operating systems make it almost impossible for IT professionals to delegate privileges to separate, task-based accounts. Rather than attempt to try to make the product use a more nuanced assignment of rights across separate accounts, it is simpler to share the same highly privileged account amongst IT professionals who need to manage the product. Taking this approach leads to issues of accountability. For example, if a group of IT professionals all share access to the same highly privileged account, it may not be clear which person was responsible for a configuration change that led to downtime.
- IT professionals log on to their day-to-day workstations with administrator, rather than unprivileged, accounts. They use that account not only to create new user accounts and install new domain controllers, but also to surf the web and check email. It's a lot simpler for an IT professional to use one account to do everything than it is to log in with a different account depending on the nature of the task that needs to be completed.
- IT professionals often circumvent organizational password policies. They use their privileges to configure the passwords on their accounts to never expire, freeing them from having to worry about changing them regularly. IT professionals find these policies as annoying as ordinary users do, but because they have administrative privileges, they are in a position to implement a work-around.
- IT professionals tend to accumulate privileges on a single account rather than have separate administrative accounts for different administrative tasks. Again this is a matter of convenience: being able to use one account for any administrative task is simpler than having to go through a process of determining which specific limited-privilege account they need to use for a specific administrative tasks.
- IT professionals often assign simple, non-expiring passwords to service accounts. This is partly a matter of simplifying things and partly a matter of not understanding that this action represents a security risk. Many successful system intrusions have started through the compromise of a service account with a simple password.
- It takes time to correctly determine which permissions must be assigned to perform a specific task. IT staff often find it simpler to over-provision accounts with privileges than

to determine precisely which privileges are required to accomplish a specific goal.

Managing Privileged Accounts

Developing a Policy for the Management of Privileged Accounts

Developing a policy for the management of privileged accounts involves balancing the needs of IT professionals, management concerns, and regulatory requirements. Only once policy objectives have been established is it possible to develop the mechanisms to implement that policy. Although the regulatory requirements for the management of privileged accounts will be region-specific, the needs of IT professionals and the concerns of management will be unique in each organization.

Although organizations will adopt unique policies, several general themes are likely to be common to all privileged account management policies. These include:

- Having concrete ways of addressing management concerns about the use of privileged accounts. Management needs to be able to quickly verify that privileged accounts are being used in a responsible manner to accomplish the organization's objectives.
- Having an effective process for overseeing the use of highly privileged accounts.
- Documenting what privileges are associated with each account. This needs to be done in a way that's transparent enough so that non-technical senior management is able to broadly understand the tasks each account can be used to accomplish.
- Reducing the complexity of privileged accounts. Each account should be associated with a small set of administrative tasks. Identifying the functionality of a privileged account must be a straightforward exercise. This benefits administrators, management, and, if necessary, third-party auditors.
- Clarifying and documenting standard administrative procedures, and having In addition, the ways of extending the documentation to provide meaningful descriptions of non-standard administrative procedures.
- Ensuring that policies are not so cumbersome that IT professionals are unable to efficiently perform the tasks associated with their role.
- Verifying that structures are put in place to meet the organization's regulatory obligations.
- Ensuring that operations that require higher levels of privilege are monitored more closely than more routine, less privileged ones.
- Guaranteeing that appropriate procedures exist to ensure that an IT professional who is no longer associated with the organization has no access to organizational resources.

Enforcing Privileged Account Management Policies

Senior management and IT professionals need to be on the same page when it comes to the oversight and administration of privileged accounts. Any mechanism used to enforce organizational policies needs to meet the objective of reliably monitoring how and when privileged accounts are used without being so inefficient as to unnecessarily hinder IT professionals in the performance of their day-to-day tasks. Such steps also need to meet compliance objectives for the management of privileged accounts.

Ideas that can be implemented to improve privileged account management in enterprise environment include:

- Ensuring that the rights and privileges assigned to individual accounts are minimized. From a practical perspective, this means that IT professionals will need to use multiple privileged accounts to perform specific tasks in the course of their day-to-day duties. It's simpler to monitor the use of task specific accounts than it is to monitor a very highly privileged account used over a large number of systems.
- Eliminating, where possible, the practice of sharing administrative account credentials among multiple people.
- Documenting the functionality of privileged accounts. This allows for checks to be performed to determine whether the account is being used in accordance with documented functionality. If an account is not being used in accordance with documented functionality, the matter should be investigated further.

- Considering account "check-out" mechanisms that require IT professional to log a request for specific administrator account credentials. This type of mechanism allows those who oversee the use of privileged accounts to see how, why, and when these accounts are being used.
- Considering mechanisms that change the password associated with a specific administrative account a certain length of time after it has been requested by the IT professional. This minimizes the chance that the IT professional can simply write down the password for the limited privilege account and uses the recorded password, rather than submitting a new request, the next time the account is needed to perform their duties.

By putting into place mechanisms to automatically manage privileged accounts, organizations can alter bad administrator habits, minimize the security risks associated with privileged accounts, and enhance the confidence senior management has that privileged accounts are being used in a responsible manner.

Benefits of Managing Administrative Privileges

Managing Administrative Privileges Enhances the Confidence of Organizational Leadership

For many in organizational leadership roles, merely knowing that a comprehensive strategy and mechanisms exist for the management of privileged accounts is likely to inspire more confidence that accounts are being used in a responsible manner. Having a process for privileged account management provides an organization with the following benefits:

- Organizational leadership will have confidence that a process will be in place to manage privileged accounts, the misuse of which could cause untold damage to the organization.
- Organizational leadership will better understand the specific tasks that are being performed by IT professionals.
- Organizational leadership will have confidence that privileges are being used in a way that is accountable.
- Organizational leadership will have faith that processes are in place to minimize the chances of a rogue employee of the IT department using administrative privileges to subvert the organization.
- Organizational management will be able to determine whether administrative tasks are being performed in a manner that meets with the organization's compliance obligations.
- Organizational management will have confidence that unusual usage of administrative privileges can be flagged so that it can be investigated later.
- Organizational leadership will have confidence that procedures will be in place to ensure that individuals who have access to privileged accounts while they are employed by the organization will lose that access in the event that their employment ceases.

Managing Administrative Privileges Improves Security

Not only does having a robust management strategy for privileged accounts enhance the confidence organizational leadership has in the way that administrative privileges are leveraged, having a robust management strategy for privileged accounts also improves organizational security. This improvement can happen in several ways:

- Minimizing the privileges associated with individual accounts minimizes the damage that can be caused if those accounts are compromised. For example, a single compromised account in a Windows-based environment that has full administrative permissions to the messaging system, SQL databases, and Active Directory can be used to cause far more havoc than a single compromised account that only has full administrative permissions to one of these critical systems.
- Ensuring that a robust privileged account password strategy is in place reduces the chances that privileged account passwords might be compromised by unauthorized people. Organizations that allow never expiring simple passwords to be used are more at risk than organizations that enforce policies where complex passwords are changed regularly.
- By limiting the practice of sharing passwords for highly privileged accounts, these accounts

are less likely to be used in a problematic way. When a group of people have access to the same account, they are less likely to be identified if the account is misused. Reducing the practice of password sharing improves accountability by tying privilege use to specific individuals.

- Tracking privilege use makes unusual privilege use more noticeable. Most attacks against organizational IT infrastructure involve unusual uses of administrative privileges. A robust privileged account management strategy makes it simpler to determine how privileged accounts are being used, which in turn makes it simpler to determine when privileged accounts are being misused.
- Having a robust privileged account management strategy makes administrators more careful about how they use their privileges and how they delegate those privileges. Someone who must regularly consider IT security is more likely to use work practices that reflect that concern than someone who views such practices as optional.
- A privileged account management process will reduce the bad habits of IT professionals, such as logging on to perform mundane tasks with highly privileged accounts. Numerous successful attacks against organizations have occurred by compromising the credentials of a highly privileged account that an administrator uses for day-to-day tasks such as checking email and surfing the web.

Conclusion

Organizations can substantially benefit by having a process in place for the use and management of administrative privileges. A robust process for the management of administrative privileges includes:

- Providing clarity on what administrative privileges are necessary
- Minimizing the use of shared administrative accounts
- Having a method of being able to verify the privileges associated with each account
- Having a method of reliably controlling and monitoring the use of account privileges

Not only will having a robust process for the oversight of administrative privileges bring peace of mind to management, it will also provide organizations with better security. Developing a robust process for the management of administrative privileges involves first developing policies for administrative privilege use and then determining the appropriate mechanisms to enforce those policies.