Mr Lech Skrajnowski

Email: Lech_skrajnowski@wp.pl

Answer to the question to check the understanding of the Minimum Least Priviledge in the Roles assignment.

The principle of the Minimum Least Privilege (PoMLP) is an information security concept that gives users, typically employees, the minimum level of access that they will need to complete their job responsibilities. CISA (Cybersecurity and Infrastructure Security Agency) recommends using least privilege as a cybersecurity best practice.

By allowing a user only the minimum level of permissions or access needed, privileged access to high-value data and critical assets is protected. This goes beyond just human users and also applies to connected devices, systems, or applications requesting access to complete a task as well.

The PoMLP has to allow the right, and minimum, amount of access while also enabling the employee to complete their job without restriction. There needs to be a balance to keep systems safe and employees productive.

Understanding minimum access policy

A minimum access policy restricts a user to only the least amount of access to privileged resources and permissions that are needed to perform an authorized activity or activities, such as those necessary for employees to do their jobs. This is a cybersecurity practice that can help to protect critical assets and sensitive data.

The minimum access policy allows a process or a user account to have only the privileges that are necessary to perform their intended function. Typically, this will mean setting the least amount of access as the default and only opening up permissions and privileges to essential resources and actions. User accounts should run and launch applications with the minimum number of privileges possible.

Understanding the Principle of the Minimum Least Privilege (PoMLP)

The Principle of the Minimum Least Privilege (PoMLP) should be a balance between security protections and usability. The user needs to have as frictionless of an experience as possible while also keeping the system as secure as possible to minimize the damage that can be caused by a mistake or malicious intent.

The Principle of the Minimum Least Privilege is a minimum access policy that centrally manages and secures privileged credentials, and only allows users access to the least amount of required privileges. It also needs to have flexible controls that can balance compliance requirements with cybersecurity, operational functions, and the end-user experience.

Benefits of the Principle of the Minimum Least Privilege include the following:

- **Reduces the attack surface**: The PoMLP limits the avenues and attack vectors that potential threat actors can use to find vulnerabilities, hack into a

system, exploit privileged information, and/or carry out a cyberattack. The broader your surface area is, the harder it is to defend against all potential threats.

The PoMLP reduces the scope of access. With fewer users having superuser or administrator privileges, for example, there are fewer possible leaks.

- **Better system stability, operational functionality, and productivity**: Applications that are running with restricted rights have less ability to negatively impact the entire system and are therefore less likely to crash the system. It can also limit the amount of downtime that occurs as the result of a potential crash or data breach. With the principle of least privilege, the system is often more stable, fault tolerance is enhanced, and work productivity can be improved.
- **Slows the spread of malware**: A PoLP can contain a threat as most users only have access to limited resources. Since there are fewer users with elevated privileges, if malware is introduced, it is easier to contain and will have more difficulty spreading throughout an entire system, wreaking havoc. With PoLP, users also have less ability to download and install unauthorized applications, which can often include malware.
- **Streamlines compliance and improves audit preparedness**: Regulatory requirements and internal policies can both require the implementation of the principle of least privilege to reduce the risk of damage to critical systems, both malicious and unintentional. PoMLP also provides an audit trail of privileged activities that can help to demonstrate compliance.

Who needs a minimum access policy?

In short, every business with digital assets or sensitive information, which is virtually any organization with a digital presence, can benefit from a minimum access policy. By enforcing the Principle of Minimum Least Privilege, you can reduce your security risk and keep critical resources and data safe. This can also help to keep business running smoothly and without disruption.

Data breaches are largely the result of human error with nearly 90 percent of data breach incidents caused by an employee’s mistake. Most of the time, this is unintentional. A minimum access policy restricts access to high-value targets to only those who absolutely need it. The fewer people with restricted access, the lower the chances of a mistake causing a security vulnerability.

Using a minimum access policy can be especially important for organizations that use contractors or third-party vendors who need remote access. The contractor will need access to specific systems and privileges to do the job being asked of them, but by using PoMLP, they are only able to access parts of the system (not the whole system), thereby reducing the potential reach of an attack.

Contractors are only granted remote access as needed. PoMLP can also utilize just-in-time access, which will revoke their privileges as soon as the job is done.

As an organization, there are often times when a particular employee will need access to different resources to complete a task and will need to be temporarily granted privileges. If these privileges are not revoked after they are no longer needed, the odds of a junior employee making a possible mistake with far-reaching systemwide consequences increase.

When many users hold administrator rights that no longer need them, this is called privilege creep. A minimum access policy can reduce privilege creep by automatically reducing access to privileges when it is no longer required — after the task is complete.

How to implement a minimum access policy ?

Using a minimum access policy, you can secure privileged accounts and credentials for machines and humans, and manage them centrally. For best practices, you will need a comprehensive access management strategy to authenticate and authorize users' access to privileged resources and systems. This will need to include policies, procedures, and tools.

To implement the principle of least privilege, use the following steps:

- **Perform a privilege audit**. You will need to audit your entire environment to find all privileged accounts. This should include both human and machine user accounts and credentials held by employees, third-party vendors, and contractors on-premises and on the cloud as well as remote access.
- **Make the default least privilege**. Reconfigure default permissions on systems or applications that allow administrator access, and remove any local administrator privileges that are unnecessary. Ensure that all users only have access to exactly what they need, which is the lowest set of privileges required to complete their job responsibilities.
- **Separate privileges and accounts**. Restrict local administrator privileges, separate administrative accounts from standard accounts, and isolate privileged user sessions. Only grant high-level functions to those who really need them and at the minimum level required. Restrict write access for log admins and host session logs outside of the database being monitored.
- **Adjust permissions as needed based on role**. *Using role-based access control, you can determine which privileges a specific task, responsibility, or team requires and set new account permissions accordingly. These permissions will need to be regularly reevaluated to help prevent privilege creep.*
- **Enable just-in-time granular access**. Use time-limited privileges or one-time-use credentials to temporarily allow a higher level of access to specific users who need elevated privileges to complete a project or certain task. Once this is complete, the credentials are revoked to avoid privilege creep.
- **Monitor and analyze privileged access.** Track all individual actions, and monitor authentications and authorizations to systems and resources across your network continuously. Watch for any activity that could potentially signal an attack to alert you to possible issues quickly.

- **Regularly review permissions and privileges.** Decide on a schedule that makes sense for the organization. Revoke privileges that are unnecessary and close inactive accounts during this review.

Summary

For the best security practices, system privileges should only be granted to those **roles** who require them. A minimum access policy ensures that users have the lowest level of privileges to complete necessary functions. One of the biggest advantages to a **minimum least privilege strategy** is the ability to lower the risk of exposure to cyberattacks and minimize any potential damage an infiltration can cause.

With the principle of least privilege, there will be fewer users with administrator access, which can make it harder for a threat actor to expose and exploit vulnerabilities within the system. Even if a lower-level user's credentials are compromised, the bad actor will only have a limited range within the system as the majority of users do not have full access. This can reduce the potential scope of a cyberattack and help to neutralize them more quickly.

A minimum access policy can help to stabilize systems, enhance functionality, and increase workplace productivity. The principle of least privilege is an important cybersecurity strategy. It is important that the minimum least privilege be balanced with usability as well.

Overall, the Principle of Minimum Least Privilege should be as frictionless for the end user as possible while still maintaining a secure environment.