Principle of least privilege

Security controls are essential to keeping sensitive data private and safe. One of the most common controls is the principle of least privilege, also referred to as PoLP or least privilege. The **principle of least privilege** is a security concept in which a user is only granted the minimum level of access and authorization required to complete a task or function.

Least privilege is a fundamental security control that supports the confidentiality, integrity, and availability (CIA) triad of information. In this reading, you'll learn how the principle of least privilege reduces risk, how it's commonly implemented, and why it should be routinely audited.

Limiting access reduces risk

Every business needs to plan for the risk of data theft, misuse, or abuse. Implementing the principle of least privilege can greatly reduce the risk of costly incidents like data breaches by:

- Limiting access to sensitive information
- Reducing the chances of accidental data modification, tampering, or loss
- Supporting system monitoring and administration

Least privilege greatly reduces the likelihood of a successful attack by connecting specific resources to specific users and placing limits on what they can do. It's an important security control that should be applied to any asset. Clearly defining who or what your users are is usually the first step of implementing least privilege effectively.

Note: Least privilege is closely related to another fundamental security principle, the *separation of duties*—a security concept that divides tasks and responsibilities among different users to prevent giving a single user complete control over critical business functions. You'll learn more about separation of duties in a different reading about identity and access management.

Determining access and authorization

To implement least privilege, access and authorization must be determined first. There are two questions to ask to do so:

- Who is the user?
- How much access do they need to a specific resource?

Determining who the user is usually straightforward. A user can refer to a person, like a customer, an employee, or a vendor. It can also refer to a device or software that's connected to your business network. In general, every user should have their own account. Accounts are typically stored and managed within an organization's directory service.

These are the most common types of user accounts:

- **Guest accounts** are provided to external users who need to access an internal network, like customers, clients, contractors, or business partners.
- **User accounts** are assigned to staff based on their job duties.
- **Service accounts** are granted to applications or software that needs to interact with other software on the network.
- **Privileged accounts** have elevated permissions or administrative access.

It's best practice to determine a baseline access level for each account type before implementing least privilege. However, the appropriate access level can change from one moment to the next. For example, a customer support representative should only have access to your information while they are helping you. Your data should then become inaccessible when the support agent starts working with another customer and they are no longer actively assisting you. Least privilege can only reduce risk if user accounts are routinely and consistently monitored.

Pro tip: Passwords play an important role when implementing the principle of least privilege. Even if user accounts are assigned appropriately, an insecure password can compromise your systems.

Auditing account privileges

Setting up the right user accounts and assigning them the appropriate privileges is a helpful first step. Periodically auditing those accounts is a key part of keeping your company’s systems secure.

There are three common approaches to auditing user accounts:

- Usage audits
- Privilege audits
- Account change audits

As a security professional, you might be involved with any of these processes.

Usage audits

When conducting a usage audit, the security team will review which resources each account is accessing and what the user is doing with the resource. Usage audits can help determine whether users are acting in accordance with an organization’s security policies. They can also help identify whether a user has permissions that can be revoked because they are no longer being used.

Privilege audits

Users tend to accumulate more access privileges than they need over time, an issue known as *privilege creep*. This might occur if an employee receives a promotion or switches teams and their job duties change. Privilege audits assess whether a user's role is in alignment with the resources they have access to.

Account change audits

Account directory services keep records and logs associated with each user. Changes to an account are usually saved and can be used to audit the directory for suspicious activity, like multiple attempts to change an account password. Performing account change audits helps to ensure that all account changes are made by authorized users.

Note: Most directory services can be configured to alert system administrators of suspicious activity.

Key takeaways

The principle of least privilege is a security control that can reduce the risk of unauthorized access to sensitive information and resources. Setting up and configuring user accounts with the right levels of access and authorization is an important step toward implementing least privilege. Auditing user accounts and revoking unnecessary access rights is an important practice that helps to maintain the confidentiality, integrity, and availability of information.