This content is part of the Essential Guide:

Advances in access governance strategy and technology

DEFINITION

principle of least privilege (POLP)

Posted by: Margaret Rouse WhatIs.com

Contributor(s): Linda Rosencrance

The principle of least privilege (POLP), an important concept in computer security, is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under POLP, users are granted permission to read, write or execute only the files or resources they need to do their jobs: In other words, the least amount of privilege necessary.

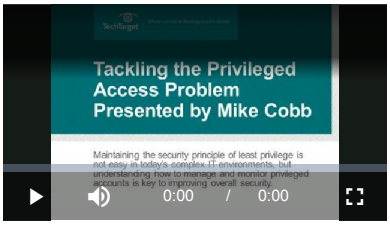
Additionally, the principle of least privilege can be applied to restricting access rights for applications, systems, processes and devices to only those permissions required to perform authorized activities.

Depending on the system, some privilege assignments may be based on attributes that are role-based, such as business units like marketing, human resources or IT, in addition to other parameters such as location, seniority, special circumstances or time of day. Depending on the operating system in use, administrators may need to tailor the different default privilege settings available for different types of user accounts.

Superuser accounts, mainly used for administration by IT staff members, have unlimited privileges over a system. The privileges granted to superuser accounts include full read, write and execute privileges as well as the ability to make changes across a network, e.g., installing or creating software or files, modifying settings and files, and deleting data and users.

Under current best practices for security, access through superuser accounts should be limited to only those required to administer systems; ideally, superuser credentials should never be used to log in to an account, but rather used with the "sudo" ("superuser do") command in Unix/Linux systems, which allows the holder of superuser credentials to issue a single command that is executed with superuser privileges. This reduces the risk of an active superuser session being hijacked.

Applying the principle of least privilege to standard user accounts means granting a limited set of privileges -- just enough privileges for users to get their jobs done, but no more than that. This type of account should be the template for ordinary employees -- least privileged users (LPUs) -- who do not need to manage or administer systems or network resources. These are the type of accounts that most users should be operating the majority of the time.



How to address the privileged user access

Watch the video and learn how to tackle the privileged user access problem.

Compared to standard user accounts, administrative accounts have more privileges and introduce heightened risk. Therefore, a best practice is to allow the administrator accounts when absolutely needed and for the shortest time necessary. This approach, known as privilege bracketing, can be used for administrative tasks as well as for ordinary users who may need elevated privileges to complete some task. Privilege bracketing can be administered using special software to automate the process so elevated access is granted only at the last possible moment and is lifted immediately after it is used. Privilege bracketing can be applied to individual users as well as to systems or processes.

Why the principle of least privilege is used

As an essential aspect of IT security, the principle of least privilege is one of the most important security policies enterprises must enforce. It is designed to improve the protection of data and functionality from faults, i.e., fault tolerance, as well as from malicious behavior. Organizations that follow the principle of least privilege ensure that users don't have more access to systems and data than they need to do their jobs.

For example, an HR staffer may need read and write access to the enterprise payroll database, but that same employee would have no need to access the enterprise client database; at the same time, an employee in the sales department would need access to the client database, but would be denied access to the payroll database.

Ensuring that employees are assigned the correct privileges prevents giving employees access to systems they don't need while also preventing malicious workers from accessing systems or data outside of their job functions. In addition, if an employee's credentials are compromised, the thief can only gain that employee's privileges.

However, the principle of least privilege isn't just about taking away privileges from users who don't need them. It is also about monitoring and managing access for those who do need access such as software developers.

Security teams should use privileged access management tools to audit their development environments to prevent privilege creep, the gradual accumulation of access rights beyond what developers need to do their jobs. Teams should also monitor when and how developers use their accounts so security information and event management tools can immediately identify irregular activity.

Benefits of using principle of least privilege

In 2016, Forrester Research estimated that 80% of security breaches involve privileged credentials. Threat actors can obtain privileged credentials and then use the access granted by those credentials to move laterally through an enterprise environment, access critical applications and systems, and maintain persistent access to the environment. However, enforcing least privilege reduces an organization's security risk and minimizes the potential disruption to the business from a security incident or data breach.

Employing POLP provides numerous benefits to organizations, starting with reducing an organization's attack surface. Restricting privileges for people, applications and processes also reduces the pathways and entrances into enterprise networks.

The principle of least privilege is also important for reducing malware infection and propagation. Applying POLP means decreasing the risk that hackers will be able to steal passwords or install malicious code that could be delivered via the web or email attachments. POLP can also help reduce the proliferation of malware because when malware infects a system strengthened by the principle of least privilege, it is often possible to contain the infection to the system where it first entered.

POLP also can help with data classification, which enables companies to know what data they have, where it resides and who has access to it, in the event of unauthorized access.

Finally, applying the principle of least privilege can help restrict hacker access. Because users will only have access to what they need, anyone who compromises user accounts will only have access to limited resources.

How to implement POLP

Organizations can maximize the odds of successfully implementing least privilege access through a variety of tactics, including:

- Conducting privilege audits by checking all existing processes, programs and accounts to ensure that they only have the permissions necessary to perform their work.
- Starting all accounts with least privilege by setting the default for all new account privileges as low as possible, and then adding higher-level privileges only as required to perform the jobs.
- Implementing separation of privileges by separating administrative accounts from standard accounts and higher-level system functions from lower ones.
- Assigning just-in-time privileges by restricting higher-level privileges only to the time when they are actually required.
- Tracking and tracing individual actions by using one-time-use credentials, monitoring and automatic auditing to make it easier to track user actions, thus enabling organizations to limit damage.

Sometimes, applying POLP may be as simple as physically removing devices or interfaces from end-user devices. For example, removing USB ports from a system can stop users from infecting their systems with USB-borne malware or exfiltrating classified information by copying it to a USB drive.

Margaret Rouse asks:

What strategies do you use to implement the policy of least privilege?

Join the Discussion

This was last updated in November 2017

Continue Reading About principle of least privilege (POLP)

- Find out how to manage privileged users in the cloud
- Read about how to prevent privilege creep
- Learn how to use the principle of least privilege to protect privileged users
- Find out how to create a data classification policy
- Learn what the U.S. Computer Emergency Readiness Team has to say on principle of least privilege

Related Terms

cybercrime

Cybercrime is any criminal activity that involves a computer, networked device or a network. See complete definition

cybersecurity

Cybersecurity is the protection of internet-connected systems -- including hardware, software and data -- from cyberattacks. See complete definition

information security (infosec)

Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect...
See complete definition

Join the conversation

1 comment

B I abc T TT H1 [CODE]

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] **Margaret Rouse**

- 26 Sep 2008 11:40 AM

What strategies do you use to implement the policy of least privilege?

Reply

SearchCloudSecurity

5 cloud storage privacy questions to ask potential providers

Data confidentiality in cloud computing is a major enterprise concern, yet providers are often lacking in their details. Here are...

Defining and evaluating SOC as a service

As cloud use increases, many enterprises outsource some security operations center functions. Evaluate if SOCaaS is the best ...

IMAGE: ISTOCK/GETTY IMAGES