SECHARD
Complete Zero Trust

Principle of Least Privilege (PoLP) Best Practices

(Tips to Implement PoLP)

www.sechard.com

→

Principle of Least Privilege (PoLP)

The Principle of Least Privilege (PoLP) is a fundamental cybersecurity concept. It dictates that users, processes, and programs should only have the absolute minimum permissions needed to do their jobs. This means limiting access to files, resources, and systems on a "need-to-know" basis.

PoLP is crucial for reducing an organization's attack surface. By restricting privileges, even if a user account or device is compromised, the potential damage is significantly contained. Malware infections are limited in their ability to spread, and both accidental or malicious insider actions are hampered.

Additionally, time-limited privileges can further enhance security. Users gain temporary access to sensitive data only for the duration needed to complete a specific task. PoLP helps prevent the creation of overprivileged users and strengthens overall security posture.

SECHARD
Complete Zero Trust

Best Practices for the Principle of Least Privilege (How to Implement PoLP)

- ✓ Conduct a Privilege Audit
- ✓ Start all Accounts with Least Privilege
- ✓ Enforce the Separation of Privileges
- ✓ Use Just-in-Time Privileges
- ✓ Make Individual Actions Traceable
- ✓ Make it Regular

www.sechard.com

✓ Conduct a Privilege Audit

Create a baseline mapping of every user account, service account, application, and system-level API with their associated permissions or roles. Understand which components have excessive access rights or no longer perform critical functions.

- **Scripting:** Develop scripts (e.g., PowerShell, Python) to pull, inventory, and parse permissions from directories (Active Directory, LDAP), configuration files, and databases.

- **Automation Tools:** Consider using vulnerability scanners or specialized Privileged Access Management (PAM) solutions to facilitate automated audits.