Principle of Least Privilege (POLP): What, Why & Best Practices

USERS ARE GIVEN ONLY THE AMOUNT OF ACCESS THEY NEED TO CARRY OUT THEIR JOBS

The principle of least privilege (POLP) is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more and nothing less.

Understandably, some end users aren't thrilled with POLP, because once enforced, it means they can no longer access certain non-essential apps, tools and networks. In some cases, it can involve removing interfaces such as USB ports from devices so that end users cannot unintentionally facilitate an infection by copying malware-laden files from a USB drive – or intentionally exfiltrate confidential information by copying it to a USB drive.

However, POLP is not designed to punish end users and make their lives more difficult. Rather, it is meant to minimize the size of the attack surface, and ultimately reduce the likelihood and severity of a cyber attack. This is especially important now that hackers routinely exploit compromised low-level accounts in order to spread laterally across devices and networks, and ultimately access critical systems and sensitive data.

ADDITIONAL BENEFITS OF POLP

In addition to minimizing the size of the attack surface, POLP offers additional security benefits, including :

- Stronger security : Before implementing POLP, organizations must first analyze current access levels for each end user. This process often reveals that many — and in some cases, most — end users have too much access in the first place, and it can be reduced accordingly. This is explored further in the "Best Practices" later in this article.

- Thwarting malware : POLP can help contain malware to a single device or to a limited number of devices, which can give security teams the time they need to investigate, contain and remediate.

- Greater stability : POLP prevents end users with relatively low-level accounts from executing changes that would affect the entire system.

- Data classification : POLP helps organizations identify what data they have in their ecosystem, where it lives, and who has access to it.

- Audit readiness : POLP significantly simplifies and streamlines the auditing process.

POLP FACTORS

Depending on the operating system, POLP can be implemented across one or multiple factors, such as :

- Role (e.g. project managers, resource managers, etc.)
- Seniority (e.g. supervisors, managers, executives, etc.)
- Business Unit (e.g. development, marketing, HR, etc.)

- Location (e.g. head office, field offices, etc.)
- Time (e.g. office hours, after office hours, etc.)

Typically, sysadmins customize the POLP profile that fits their organization's specific needs, and seek to balance the need for strong security with the fact that end users require sufficient access to be productive and efficient.

POLP BEST PRACTICES

There are a number of POLP best practices that organizations are strongly encouraged to adopt — and not just big enterprises, either. SMBs have become "ground zero" for cyber crime, and a staggering 60% of small businesses go out of business altogether within six months of a major cyber attack. These best practices include :

- In consultation with end users (a.k.a. business owners), evaluate each role to determine the appropriate access level. Make "least privilege" the default starting point, and add higher-level access as needed.
- Communicate the purpose of POLP to all end users — including the serious costs and long-term damage of a major hack — so they understand that the approach is not intended to stifle their productivity, but rather to protect the organization (and at the same time safeguard their job !).
- When temporary privileged access is required, use one-time-use credentials that are granted at the last possible moment, and which are then revoked immediately after use. This approach, known as privilege bracketing, can be used for individual end users as well as processes or systems.
- Separate administrator accounts from standard accounts.
- Separate higher-level system functions from lower-level system functions.
- Automatically track all logins and activity; it is very important to have full visibility to see exactly what end users do and when.
- Regularly audit end user privileges to ensure that access is appropriate. This includes removing access for all employees who have left the company.
- Have a way to automatically revoke privileged access in the event of an emergency.

HOW DEVOLUTIONS PASSWORD SERVER HELPS

Devolutions Password Server (DPS) can be an important piece of the overall POLP puzzle. It securely and centrally empowers organizations to :

- Establish enterprise-wide role-based access to privileged accounts and critical assets.
- Set customized granular and global permission settings.
- Centrally control privileged access management logs.
- Ensure that only authorized sysadmins can grant privileged access.
- Hide privileged credentials from users and prevent them from reaching endpoints.
- Store all usernames, credentials, and privileged account access in a centralized vault that is protected by U.S. Federal-government-approved encryption.

In addition, when integrated with Remote Desktop Manager (RDM), DPS supports one-click direct connection to websites, apps and remote IT resources, providing a simplified and highly secured remote access management. It also features an easy-to-use and simplified web interface for end users to store passwords and other confidential information.

THE BOTTOM LINE

At the 2017 Black Hat conference, privileged account solutions company Thycotic conducted a survey of more than 250 self-described hackers who revealed that the number one way to get hold of sensitive data is by hacking privileged accounts. And according to the Verizon 2017 Data Breach Investigation Report, a whopping 81% of breaches derive from stolen, default or weak passwords. Add it all up and it means that POLP is not just a smart idea, but it is essential on an increasingly threatening landscape where the risks and costs of a breach are getting higher and higher.