ManageEngine
PAM360

How should you manage your privileged users?

Paul Edwards

www.manageengine.com/pam360

Privileged users are those who are authorized (and trusted) to perform security-relevant operations that ordinary users are not authorized to perform. Privileged user access management (PUAM) is perhaps the most difficult part of a comprehensive information security and cybersecurity strategy to implement. A subset of privileged access management, it has more impact on frontline users than most other aspects of cybersecurity. It's a discipline where there are more areas of gray, and an incorrectly calibrated approach to PUAM can have repercussions throughout an organization. How should an organization manage its privileged users?

Why is managing privileged users important?

To answer this question, we first need to understand what we mean by privileged users. When viewed through a technology lens, a privileged user is typically a user with administrator access. The level of access may be either on a single device (a workstation, a server, or a switch), or at a domain level.There is another type of privileged user to be considered when thinking about managing privileged users: a user who is privileged via a business process. For example, a user might have access to approve spending in the finance system, have access to the personally identifying information (PII) of staff members, or have access to a key business system. A common example is a bank employee who has access to the SWIFT system that facilitates international interbank payments. A SWIFT users' credentials command a premium bounty on the dark web. Whether accidental or malicious, misuse of the privileged users' rights may lead to theft of funds; theft of PII; attacks from within on the reputation of the organization; alterations of logs to make detection more difficult; use of the organization as a staging ground for a bigger attack; and more.

Business and technology privileged users are an inherent source of weakness for organizations, yet paradoxically are essential for the organization to operate. The question is: what is the best way to manage privileged users?

Option 1: Go loose

The first option is to put PUAM into the "too-hard basket", and not attempt to manage privileged user access at all. I've seen this approach in too many companies—more than I care to remember. These are not "mom-and-pop" businesses—one had over 200 employees, where everyone had administrative access on their laptops, and the only control on the finance system was whether you had access to it or not. The usual reason given for this approach is cost or complexity. Granted, achieving PUAM is difficult. If an organization chooses not to implement an approach to PUAM, there are a number of mitigating controls that can be put in place.

Here's a short list of technical controls:

- A heavily micro-segmented network that halts lateral movement.
- Extensive and highly restrictive data loss prevention (DLP) and data classification solutions.
- Employee and contractor agreements that enforce penalties for the misuse of technology assets. The challenge here is to determine whether the intent was malicious or accidental.
- Cyber insurance.

The expense of executing these should be compared to the cost of implementing a carefully thought through approach to PUAM. These technical controls, plus others, would be part of any comprehensive information security strategy, but not necessarily implemented to the depth required to mitigate against the absence of PUAM.Imagine having this policy in the business side. Everyone would have unfettered access to customers, HR, and finance systems. What could possibly go wrong?

Option 2: Go tight

In this scenario, there are very few people within the organization who have privileged access. I've seen this approach in numerous companies—especially in government organizations, although not military. This is based on the centralized model used in the days of large central computers: a small number of systems administrators had privileges to perform system administration tasks, and a large number of non-privileged users consumed the system resources.This approach seems to solve almost all of the problems in the first option. Users wanting elevated privileges (technical or business) need a clear justification for the requested access. All privileged access is logged, and carefully audited for misuse. Lateral movement becomes extremely difficult. Genuine mistakes by the staff don't result in the consequences they otherwise would. Bad actors simply look elsewhere for an easier target. This is not as rosy as it seems. A reasonably large company that I recently consulted for had just attempted adoption of "Go tight" and was in the process of unwinding it. The company had 600 applications on 50,000 workstations and 20,000 production servers, all managed by approximately 8,000 technology staff. The organization's directive was that no more than 1% of the technology staff, about 80 members, should have privileged access.

Viewed through the lens of change management, this presented challenges. A typical weekend in this company involved over 400 changes to its infrastructure, and most required privileged access. This heavy workload for 80 in the IT department frequently led to burnout.

Or, consider the service desk. Implementing this approach, only six of the service desk staff had administrative access to make changes on end user workstations. Any end user problems that required remote administrative access was run through them.

Unsurprisingly, the backlog of issues grew, and frontline staff productivity plummeted as these six staffers worked through the queue. The "only six service desk staff to have admin access" edict was rolled back after the second day.Similar problems exist from a business perspective as well. Suppose the organization only allows a small number of people to approve payments as a means of managing privileged user access. Accounts payable will quickly grind to a halt with a massive backlog.

Option 3: Go Goldilocks

As with most choices, extremes are not desirable, and somewhere in between provides the optimal solution. Precisely where to position an organization is difficult! There are multiple tactical approaches that can be applied independently to help build an overall strategy. Some of the more common areas to consider include:

The least privilege principle: Determine the lowest level of privilege needed for each user in their role. This approach scales well, as it's possible to establish the least privilege required for a class of user, and apply that level to all users who are members of that class.

Temporary elevation of privileges: For specifictasks, users are able to receive a temporary elevation of privileges. Examples of this include the earlier change management situation: appropriately skilled people can be recruited to provide temporary help to make these changes. A business side example of this would be when a person goes on a planned absence, and their tasks and associated responsibilities are delegated to someone else.

Granular privileges: This is a specialized instance of the least privilege principle. Consider assigning administrative access at a local level only, rather than at a domain level. For example, a Unix administrator cannot

manage a Windows server, and vice versa. Or, a bank teller may be able to access the retail banking system, but not the institutional banking software. Adopting the Goldilocks approach is not without issues, nor is it foolproof. The increased complexity leads to a requirement for greater planning, careful management of processes and exceptions, and additional audit requirements. There have been countless examples of senior executives getting spear-phished and conned into approving the transfer of moneyto criminals; employees who have addictions of various types bypassing controls and defrauding companies; and attackers having an armchair ride in exfiltrating data due to unnecessary privileged accounts, despite the organization's best effort at tuning their approach.

Summary

In summary, it's possible to take a more laissez-faire approach, or what we have called "Go loose". Things happen quickly, including getting that new dev platform installed on developer machines, account invoices being paid, and that dodgy copy of office productivity applications. What also goes fast is the company's bank balance, customer data onto the dark web, and reputation in the eyes of customers (former and potential), regulators, and shareholders.

Organizations can also take a tighter approach, which massively reduces the risk of any of the issues of the "Go loose" model occurring, but at the expense of organizational efficiency and actually getting issues resolved or invoices paid in a timely fashion. Finally, there's the recommended approach: the Goldilocks approach which attempts to take the best of both worlds.

How much of each world an organization wishes to take depends on several factors, including its risk appetite, the level of regulation, and how much it's willing to invest on mitigating controls to ensure it maintains that

balance between freedom and security. Time is a factor too. Organizations should consider the speed of business processing required to be competitive, and how quickly it requires technology incidents to be resolved and changes implemented.

To achieve the best outcome for PUAM, the inherent tension across multiple dimensions must be resolved. PUAM is not easy. That is because PUAM is not about finding the right outcome; it's about finding the least-worst outcome for the organization and its context.

About the author:

Paul Edwards

Paul has been involved with cyber security in both policy and operations roles in the higher education and financial services sectors in Australia since 1998. As part of those roles, Paul has advised on the development of government regulation with regard to cyber security, appeared as an expert witness in court, and has held a variety of senior and executive cyber security roles in three of Australia's largest banks and insurance companies. Paul was responsible for building a Security Operations Centre for a major Australian bank which subsequently won industry awards for both the speed of implementation as well as its world-class effectiveness. In addition to his work in cyber security, Paul has spent time working as an ITSM consultant, as a programmer on supercomputers, and is an accredited coach with the International Coaching Federation.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360