The Critical Importance of Privileged Identity Management (PIM)

Devolutions

WAYK NOW IS OUR, POWERFUL, LIGHTWEIGHT AND EASY-TO-USE REMOTE ACCESS TOOL

As security and risk management (SRM) professionals know — and sometimes have a difficult time getting end users, customers, and other stakeholders to understand and accept — the most important piece of privileged identity management (PIM) is not identity or management: it is **privileged**.

This is because the heart of a robust and functional PIM system is determining who should — and just as importantly, who should not — have administrative access to critical systems, since access often users the ability to access secure data, change configurations, install software, modify accounts, and so on.

Naturally, all end users want "super user" designation because it makes their lives easier. It is like having a master key that can unlock any (virtual) door. However, granting privileged status to the wrong users — and for the wrong reasons — also makes things much easier for hackers. In fact, in the Forrester Wave™: Privileged Identity Management, Q4 2018 Report, Forrester estimates that a whopping 80% of data breaches can be traced back to compromised privileged credentials such as passwords, tokens, keys and certificates. Indeed, it is alarming how simple it is for cyber criminals to grab Windows administrator and Unix root credentials, and then move laterally across systems and devices.

4 Reasons PIM Is Crucial

As highlighted by Forrester in the above report, there are four key reasons why PIM must be a crucial part of an organization's security profile — including SMBs, which are increasingly becoming ground zero for cyber crime. These four reasons are:

#1. PIM helps thwart would-be hackers from getting a foothold into networks and launching full-scale attacks — including some that persist for prolonged periods of time. A study by IBM found that the average time to detect a data breach is 197 days, and it takes an additional 69 days to contain it and clean it up.

#2. PIM governs and safeguards the interaction between customer identity and access management (CIAM) portals and customer relationship management (CRM) systems. For years, hackers have been targeting vulnerabilities in this integration to snoop and steal privileged credentials.

#3. PIM helps keep hackers from gaining access to privileged database credentials, which can be catastrophic. Just ask Equifax, which in 2017 was the victim of a mega-hack that exposed the confidential information of more than 150 million clients worldwide. The situation was so chaotic that according to a recently-released report from the U.S. Government's Accountability Office (GAO), Equifax's IT staff spent weeks re-running the hacker's own database queries just to find out what was stolen!

#4. PIM secures and protects containerized and cloud environments, which require administrator keys to function and share information. To that end, products such as Azure AD support custom role assignments for various tasks.

PIM Best Practices

Mismanaging access to privileged accounts — or failing to manage them at all, which is something that a staggering 65% of organizations are guilty of doing — can lead to everything from security breaches and regulatory penalties, to customer revolts and lasting reputation damage. In some cases, it can even lead to extinction: a study by the National Cyber Security Alliance found that 60% of SMBs go out of business within six months of a cyber attack.

This means that establishing, executing and evolving a robust PIM system is not an option. Organizations of all sizes must make it a top priority, or else it is arguably not a matter of when they will be under attack, but a matter of how severe the attack will be. To guide security and risk management professionals, Gartner and Centrify have teamed up to highlight best practices for establishing a comprehensive PIM system. These include:

- Identify and analyze all privileged accounts and end users to ensure that access is appropriate, aligns with acceptable risk levels, and complies with regulatory requirements.
- Ensure access to privileged accounts complies with the principle of least privilege principle (POLP), which gives end users only as much access as required to perform their jobs — and nothing more.
- Constantly monitor all privileged account usage and enforce strict controls for sharing credentials.
- Implement high-trust authentication methods for privileged access, and leverage suitable PIM/PAM tools and technologies. Devolutions is one of a select list of vendors that has been identified by Gartner analysts as effectively delivering an alternative way to mitigate the risks around privileged access, or providing a set of specific and deep capabilities to augment existing PAM deployment.
- Augment and extend privileged identity management with access governance controls to meet ongoing compliance needs (e.g. requiring account owners to certify that they still require privileged access after a period of time).

From Devolutions' Chief Security Officer

Here is what our CSO Martin Lemay advises:
PIM is an excellent solution to prevent excessive privilege scenarios by reducing opportunities for an attacker to compromise privileged access. However, an effective Segregation of Duties (SoD) must also be considered to avoid giving certain users "too many hats" to wear at work — which could expose the business to a wide range of threats. If any of these users are compromised, then hackers can access all of their accounts. Similarly, when multiple individuals have tasks that overlap with each other, if one of them gets compromised then that will most likely expose privileged access to systems.

Your Advice

What PIM best practices are you following — or advocating for — in your organization? What strategies and tactics have worked for you, and what has proven to be ineffective, or maybe even disastrous?

Please share your insights below so that together we can all be part of the PIM solution, staying a step or two ahead of the bad guys.

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.