Is It Time to Rethink Privileged Access Management?

Devolutions

PAM IS ESPECIALLY VITAL THESE DAYS

Privileged Access Management (PAM) helps organizations achieve two key objectives: **restricting access to privileged accounts and maintaining compliance.**

PAM is especially vital these days because, in many organizations, the number of user accounts with administrative access to critical systems is greater than the total number of employees.

What's more, 8 out of 10 breaches are facilitated — intentionally and unintentionally — by internal users. Read this article to learn more about the 4 most common ways that insider leaks happen.

A PAM SOLUTION HAS THREE CORE COMPONENTS:

- **Access Manager:** This involves creating policies for groups of users, and setting various rights, permissions and restrictions for these groups.

- **Password Vault:** This enables privileged users to create strong passwords and securely store and access them. For enhanced security, passwords can be completely hidden from users.

- **Session Manager:** This tracks what privileged users are doing during an administrative session.

Frankly, there is no 100% bulletproof way to stop cyberthreats. As noted in Forbes: "The sheer complexity of IT systems and human nature means that intrusions may be all but certain for every organization." As such, ultimately a PAM solution is all about identifying, managing and mitigating risk — and lowering the chances that an organization will get victimized by an attack.

What We Need to Rethink About PAM

IT pros are starting to sound the alarm bells and warn their superiors that a growing number of users outside of the IT environment are being granted access to privileged accounts — and while this may enhance productivity and be more convenient, it's also a significant risk. And so, one of the things that we need to rethink is **who truly is a privileged user — and who isn't.**

In the past, this wasn't a difficult challenge. Privileged users were typically CTOs, CIOs, Sysadmins, and other managers and leaders in the IT environment. But today, C-level executives, managers and team leaders from other departments and divisions (e.g. operations, R&D, sales, etc.) want and expect access to data and assets that are only accessible through privileged accounts.

And guess what? While most hackers aren't the ultra-high IQ wizards that the media often portrays them to be, they certainly aren't stupid! They see this shift, and are targeting non-IT users who don't know — or don't care — about following strong password management and infosec policies. For example, hackers hit the jackpot when they discover that a marketing manager is using the same password for multiple accounts. The long-term financial and reputation damage hackers can unleash in a matter of minutes is staggering.

Another thing we should rethink is **who should use a PAM solution**. In the past, it was assumed that only large enterprises needed to have something as sophisticated as a PAM solution, while SMBs would be fine with traditional tools (e.g. firewalls, secure web gateways, anti-virus software, etc.). However, SMBs are becoming the primary target of hackers. Indeed, as we've highlighted previously: size doesn't matter for cyber criminals.

Of course, SMBs typically don't have the resources or the personnel to implement the same kind of PAM solution as a unicorn like Google or Apple. And that means the marketplace needs to close the gap and provide SMBs with PAM solutions that fit their needs and budget; not one or the other.

Devolutions Is Part of the Solution

Devolutions is proud to be part of the PAM solution for organizations of all sizes, including SMBs. For example, **we were selected by Gartner** as one of a small list of vendors in the world that effectively delivers an alternative way to mitigate the risks around privileged access. As noted by Gartner analysts: "Devolutions offers Devolutions Server, Password Vault Manager and Remote Desktop Manager. The combination of these products offers capabilities for vaulting administrative passwords, account sharing and session management." Click here to learn more about the role our products play in a comprehensive — and affordable — PAM solution.

What's Your Take?

How is your organization leveraging a PAM solution to address the growing risk of insider threats? What are your best practices and biggest warnings? Please share your experience and wisdom with the community.