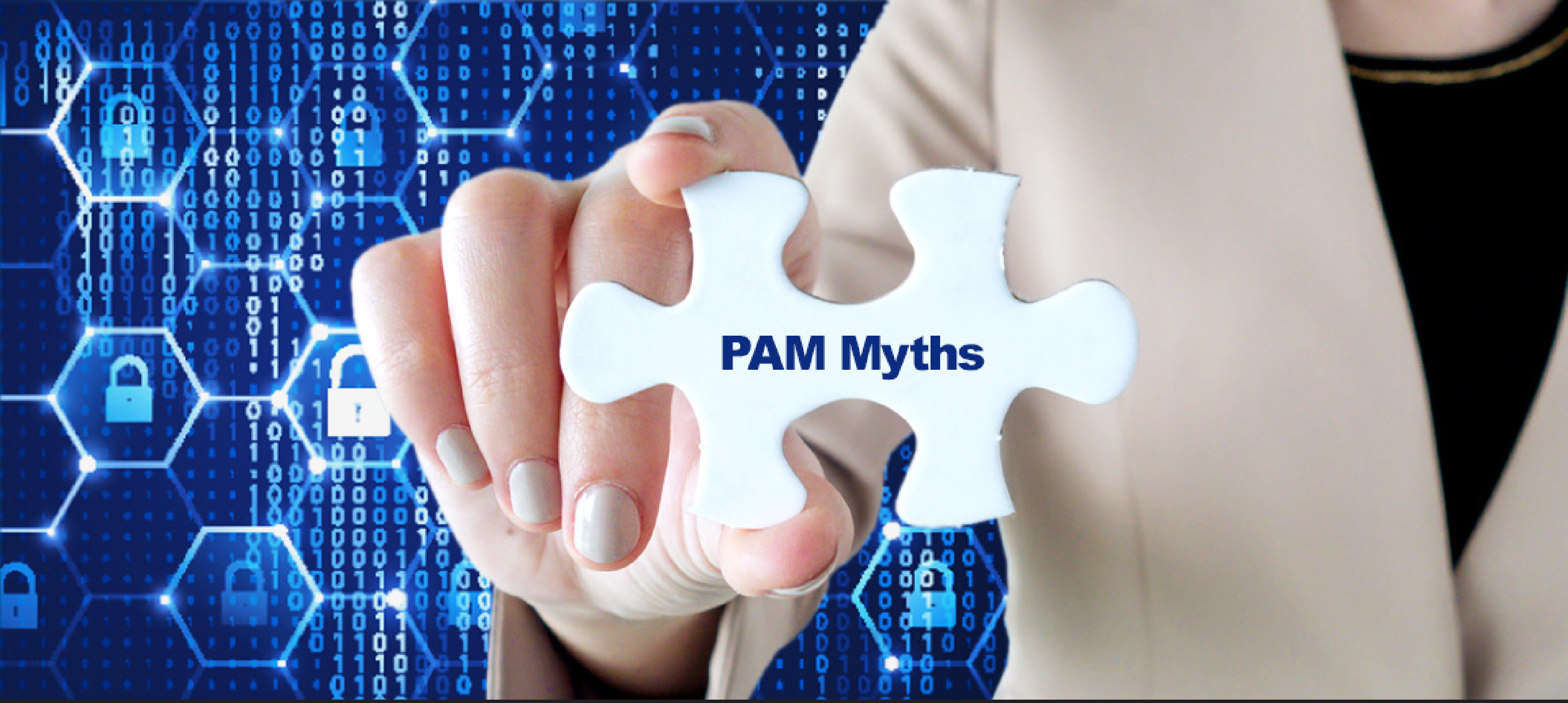

Debunking 6 Myths About Privileged Access Management

Devolutions

SOME MYTHS IN LIFE ARE DANGEROUS AND HAVE THE POTENTIAL TO BE VERY COSTLY

Some myths in life are harmless, or even charming and helpful — like Santa Claus and the Tooth Fairy (sorry if we're shattering anyone's fantasies with this revelation). But some myths in life are dangerous and have the potential to be very costly — or in some cases, catastrophic.

Unfortunately, six enduring myths about Privileged Access Management (PAM) fall into the latter category and make this list. Here they are:

Myth #1: You don’t need to worry about PAM if you have advanced network security tools in place.

Truth: It’s obviously important to implement advanced network security tools, such as firewalls, intrusion prevention systems, antivirus and antimalware software. But believing that this is enough is a major mistake.

Why? Because a staggering 81% of hacking incidents involve stolen or weak passwords. And once cyber criminals get their hands on passwords — they particularly enjoy grabbing compromised Windows administrator and Unix root credentials — they unlock the virtual door to steal data, commit identity theft, and damage reputations.

Myth #2: You don’t need a PAM solution if you regularly rotate passwords.

Truth: In the past, rotating passwords — i.e. making end users change them every few months or once a year — was a best practice. But sometimes best practices turn out to be bad advice (like how smoking cigarettes until the 1950s was approved and endorsed by physicians).

Yes, in theory rotating passwords makes sense. But research has shown that instead of choosing strong passwords, end users head in the other direction: they choose weaker passwords. That’s bad news for organizations and great news for hackers, who probably spend a lot of their day shaking their head in awe and saying: “I can’t believe how easy they’re making this”.

And what’s more, even if some end users do choose strong, long and unique passwords — or better yet, passphrases — this doesn’t replace a comprehensive PAM solution, which (among other things) includes password vaulting, automatic logging, and other key security and governance functions.

Myth #3: If you haven’t been hacked (yet) due to compromised credentials, then you must have some kind of functional PAM solution in place.

Truth: Logicians call this kind of reasoning spurious. Hackers have another name for it: “wonderful” — because it makes their job even easier. Here’s the cold, hard truth: if you don’t have a PAM solution in place, then you don’t have a PAM solution in place. It doesn’t spontaneously create itself using different parts and pieces, like some kind of magical Autobot (“Freedom is the right of all sentient beings” — Optimus Prime).

In fact, 55% of businesses have no idea how many privileged accounts they have or where they are located, more than 50% of businesses have privileged accounts that never expire or get deprovisioned, and 82% of businesses fail to store all of their privileged accounts in a secure manner.

Myth #4: If you implement a PAM solution, then you'll also need to implement Zero-Trust Architecture, Segregation of Duties (SoD) and Principle of Least Privilege (POLP) — and your end users will revolt.

Truth: Do you know what irritates end users even more than requesting access to certain accounts or areas of the network, or being obligated to share passwords through a secure platform instead of email or text? Losing their job because their company was hacked and must spend hundreds of thousands (or maybe millions) of dollars to investigate, remediate and repair the damage.

Of course, moving to a Zero Trust architecture environment, establishing Segregation of Duties (SoD), and implementing the Principle of Least Privilege (POLP) is a process that takes time — and there will be obstacles along the way that put leadership, IT and end user patience to the test. But it is well worth the effort given what's at stake. The key is to educate end users and hold them accountable, so that they play an active role in being part of the security solution — instead of playing a passive role and remain part of the security problem.

Myth #5: PAM is for large organizations, not for small and mid-sized businesses (SMBs).

Truth: SMBs have become ground zero for cyber crime, and poor user password hygiene is the top cause of SMB hacks. And if that wasn't frightening enough, then consider this: 60% of small businesses fold within six months of a cyberattack. The moral to this horror story? A PAM solution isn't optional for SMBs: it's essential. Hackers don't need much more than a single compromised set of credentials — or a brute force attack that cracks a password — to wreak costly havoc. And that brings us to the last myth, which is also about SMBs...

Myth #6: Comprehensive PAM solutions are too expensive for SMBs.

Truth: OK, this isn't a complete myth. Or to put it differently, it's partially true. Yes, traditionally, PAM solutions are quite expensive and beyond the financial reach of many SMBs — which is deliberate, because the intended targets are large organizations with 6- and 7-figure annual InfoSec budgets. But this doesn't mean that all PAM solutions are unaffordable, or that they are excessively complex to implement and manage.

At Devolutions, we are on a mission to solve this major problem faced by SMBs. To that end, we have worked closely with two well-known analyst firms, and we are on target to deliver a robust, affordable, and easy-to-implement PAM solution that is specifically designed for SMBs by November 2019. Learn more here.

From Our CSO Martin Lemay:

Another myth I often hear is: "If you have nothing exposed to the Internet, you don't have to worry about cybersecurity risks". The truth is that 15% of threats, according to a recent ISACA study , are from non-malicious insiders, and 13% are from malicious insiders. This fact must be considered when performing your annual security risk assessment. PAM solutions can help prevent unauthorized access not only from outsiders, but insiders as well. They provide useful audit and monitoring functionalities to detect unusual and malicious activity.

The Truth Will Keep You Safe

It's been said that the truth will set you free. But in the context of busting these six PAM myths, the truth will help keep your company safe from data hacks and breaches — which is just as liberating and rewarding!