The Enemy Within: 72% of IT Pros Admit They're Vulnerable to Insider Threats

Devolutions

72% OF IT PROS ADMIT THAT THEIR ORGANIZATION IS VULNERABLE TO INSIDER THREATS

The most chilling horror movies are never about threats that strike from beyond. They're about dangers that lurk within — in the basement, the attic, or the TV ("they're heeeeeeeeere"). Well, IT pros can be forgiven for lying awake in bed at night clutching the sheets — not because they're petrified of demonic possessions or poltergeists, but because they're terrified of end users.

A recent survey by security and fraud analytics firm Gurucul revealed that 72% of IT pros admit that their organization is vulnerable to insider threats — and 11% say they are "exceedingly vulnerable". Other scary revelations include:

- The biggest source of fear are user errors (40%), followed by malicious insiders (35%).
- Companies in the tech sector worry the most about malicious insiders, while those in the retail space worry the most about user errors.
- 74% of IT pros cannot detect an insider threat before data exfiltration.
- 64% of IT pros cannot detect an insider threat in real-time.
- 61% of IT pros are not monitoring privileged and service accounts.

While all of these statistics are distressing, in our view the most alarming is the last one: 61% of IT pros are not monitoring privileged and service accounts. These accounts are widely understood — not just by IT pros, but unfortunately by hackers as well — as the "keys to the corporate crown jewels". Once they are compromised, bad actors can steal data, commit identity theft, and establish a foothold to launch persistent campaigns across multiple devices and networks. According to a survey by security service platform provider Centrify, a whopping 74% of data breaches begin with privileged credential abuse.

In light of this massive security gap, it's not surprising that PAM is #1 on the list of Gartner's Top 10 Security Projects for 2019. Gartner analysts advise that PAM projects should include both human and nonhuman systems and accounts, and they should support a mix of cloud, on-premises and hybrid environments, along with APIs for automation.

While Gartner's advice is certainly valid, the problem is that current PAM solutions in the marketplace are very expensive and beyond the budget of most small and mid-sized businesses (SMBs). What's more, the small percentage of SMBs that can afford a PAM solution typically lack the in-house technical expertise to understand the differences between core and non-essential requirements. **At Devolutions, we are on a mission to change this, and we're on pace to launch a robust and fully-featured PAM platform specifically designed for SMBs by November 2019! Learn more here.**

From the Desk of Our CSO Martin Lemay

While technology can help prevent, detect and respond to insider threats, many organizations are not considering non-tech controls. For instance, a periodic criminal background and credit check performed by human resources will greatly prevent high-risk individuals from accessing sensitive data and mission-critical systems in your organization. The cost of such control is far cheaper than buying any tech

solution. Other useful controls driven by Segregation of Duties (SoD) and the principle of least privilege (POLP) do not require specific technology either. These principles can considerably lower the attack surface and limit undesired actions from malicious and non-malicious employees. Another neglected topic is the four-eye principle enforced by strong change management and audit processes. This last recommendation will not only help prevent, but also leverage, detection of potential abuse and misbehaviour. Finally, I'd like to add that defence in depth should be leveraged by combining both technical and non-technical controls in order to limit insider threat occurrences and impacts.