The importance of **privileged access security**

Agencies need targeted solutions to prevent hackers from compromising high-level credentials

Kevin Jermyn
Regional Manager of Federal Customer Success, CyberArk

A BUSE OF PRIVILEGE is at the heart of almost all cyberattacks. Because the government holds sensitive information whose loss could undermine national security or public safety, it's crucial that agencies have a strong program to control, manage and monitor privileged access to critical assets.

One key component is the ability to restrict a hacker's access as soon as an attack is detected without negatively affecting legitimate users' abilities to meet their goals or missions.

To accomplish this, agencies need to take a programmatic approach to prioritizing risk and securing the most common privileged pathways that attackers seek to abuse, such as built-in admin accounts, unmanaged service accounts and highly privileged user accounts.

4 steps to limiting the risk

Agencies can take several steps to mitigate the risk of insider threats and external attackers. The first is to minimize user privileges wherever possible to reduce the attack surface.

Next, agencies should centralize access to critical infrastructure by storing privileged credentials in a secure repository with strong access controls, multifactor authentication and full auditability so that administrators know who is doing what. These credentials should be rotated on a regular basis.

Third, agencies can limit the power of any one account by segregating administrative duties and controlling role-based access. Following the least-privilege principle ensures users have access to what they need to fulfill their roles and responsibilities, but nothing more.

Finally, agencies should monitor and analyze the behavior and activities of privileged users to learn what's normal and more easily identify anomalies. If someone who typically accesses a system during business hours suddenly logs on at 2 a.m., that activity should trigger an alert and a response to block the potential attack.

Privileged access and the cloud

When agencies move to the cloud, the focus shifts from securing a server connection to securing a connection to a web console, command-line interface or machine application. Each of those tools has its own version of role-based access and admin controls, but the systems don't work well together and don't provide a centralized audit record of privileged access.

As agencies migrate to the cloud, it's important to avoid creating technical debt by adopting the easiest option now with the intention of reworking it later to meet specific needs. The better approach is to define a centralized structure from the beginning that incorporates best practices for managing privileged access.

Comprehensive privileged access security for systems and data both on-premises and in the cloud is critical to reducing risk, meeting compliance requirements and improving operational efficiency. ■

Kevin Jermyn is regional manager of federal customer success at CyberArk.