Making the most of privileged access management

To maximize security and effectiveness, agencies must first define what desired user activity looks like

The identity and access management landscape is broad, spanning everything from onboarding and offboarding employees to derived credentials, access for automated processes and continuous multifactor authentication.

"When we talk about monitoring identity within an organization, we have to model what their behavior truly is," said Morey J. Haber, CTO and CISO of BeyondTrust. The purpose of this modeling is to understand the context and parameters of appropriate use, and anything done inappropriately before, after, or during the session, he said

To meet these challenges in alignment with the CDM Program, Haber recommended taking an identity-centric approach. "If we start with the identity piece and get a better handle on who people are, what they're doing, and the privileges they're supposed to be using," the enterprise can get relevant, reliable information to the CDM dashboards.

The goal is visibility in the service of proactive control, detection and intervention. "You can't manage what you can't discover and monitor," he said. BeyondTrust is an IAM company with clients across the federal sector.

The solution set he advised is based on a refined IAM process for visibility into user access, legitimate tools and strong governance. An accurate perspective of monitoring and diagnostic behavior—what the end user is doing—requires an understanding of three key facets: asset, privileges, and identity.

Privileged access management is one of the most important factors in this equation, and it is imperative that PAM strategies and tools are effective. Privileged accounts have access to the most sensitive systems and are enabled to do configuration, updates, administration and other changes; they can exfiltrate data en masse, or plant malware, he explained.

Since the COVID-19 health pandemic and the massive pivot to remote work, organizations have had to shift perspective in order to know how people are using their systems, and across all of their assets and the privileges assigned.

"Think of all the users you have out there and the various accounts that they may be mapping to. … The model is fairly straightforward; it's the people we worry about. Something intentional or unintentional that poses risk—that's the type of awareness we need to bubble up through CDM," he said. Haber's expertise includes attack vectors and threat mitigation.

IAM is only one small bucket in data security, he said, urging organizations to consider the rest of the model, for example network and IOT devices and different types of parameters. The data is what matters, he said: "We need to protect the privileged accounts that can see, operate, and manipulate data," for endpoint access and servers.

PAM provides a rich set of data to the elastic search dashboards, with indicators and evidence of compromise. Enhanced understanding of where assets are, where users are, and accounts associated with users and identity are mapped, which helps eliminate shadow IT and supports timely and accurate data going to that dashboard.

From a foundational standpoint, he said, any solution has to allow for context, which means a comprehensive dashboard and providing consistency for user experience. "Let the people worrying about managing privileges see it in their context, in their view, then escalate the proper information to the higher-level elastic search dashboards, where it can be corroborated with other information, run through AI/ML, used with the AWARE algorithm, and other places that make a big difference for the organization," he explained.

"When we talk about monitoring identity within an organization, we have to model what their behavior truly is."

– MOREY J. HABER, CHIEF TECHNOLOGY OFFICER, CHIEF INFORMATION SECURITY OFFICER, BEYONDTRUST

Industry standards—the SCIM, or System for Cross-domain Identity Management, specification is one example—facilitate transfer of data between vault technologies like Password Safe and similar tools so the associated entitlements can be visible and managed throughout the identity governance process.

Active directory tools—ADBridge is one of BeyondTrust's technologies—enable capabilities such as system integration, single sign-on and password storage, and reduce the risk of credentials being misused.

"IAM is only one small bucket in data security," Haber said. Data is the usual objective of threat actor attacks. Because PAM is crucial for those accounts that can see, operate and manipulate data, he urged organizations to consider all aspects of the model, and for endpoint access and servers—pointing out as examples network and IOT devices and different types of parameters.

"The last thing we want is a cybersecurity tool that we've implemented [that is] providing us with good data [and] good blocking … to be compromised and leveraged against us," he said.

Article Source: FCW CDM Summit | November 19, 2020