Government Business Council

PRIVILEGED ACCESS MANAGEMENT IS ESSENTIAL TO ZERO TRUST

A CANDID DISCUSSION WITH GOVERNMENT CYBERSECURITY EXPERTS

EXPERT DIALOGUE

BeyondTrust

INTRODUCTION

Effective cybersecurity has become exponentially more important as cyberattacks grow both in number and sophistication. Recent attacks targeting U.S. critical infrastructure and national security systems demonstrate the severity of cyber threats and have brought forth the White House Executive Order on Cybersecurity, which requires agencies to move towards a Zero Trust security posture. Protecting data from malicious actors has become a national security concern.

One potential pathway toward enhanced cybersecurity is the use of privileged access management (PAM) solutions. PAM enhances cybersecurity by enforcing least privilege access controls to ensure only the right users have access to the right data at the right time. The principal of "never trust, always verify," has become critically important to address the access and usability demands of modern users, while protecting agency systems. To better understand the government cybersecurity landscape, and how privileged access management mitigates risk, GBC interviewed the following experts:

EXPERTS

Mike Witt

Senior Agency Information Security Officer and Chief Information Security Officer
National Aeronautics and Space Administration

Mike Witt is responsible for implementing NASA's Cybersecurity Program and providing guidance and assistance to the Administrator, the NASA CIO, Center Directors, Mission Leadership and other senior Agency personnel with IT roles and responsibilities. Mike also interacts with external groups regarding cybersecurity, including OMB, DHS, Congress, other Federal agencies and entities exhibiting cybersecurity best practices and plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize cybersecurity risks.

Gerald Caron

Chief Information Officer / Assistant Inspector General for Information Technology
U.S. Department of Health and Human Services, Office of the Inspector General

Gerald Caron is a senior executive in the federal government with 20 years of experience from the Department of State. As the CIO, Gerald is responsible for all things cybersecurity, including risk acceptance as well as IT operations and modernization efforts.

Jeremy Wilson

Deputy CISO for Security Operations
State of Texas Department of Information Resources

Jeremy Wilson is responsible for overseeing the State of Texas Regional Security Operations Center (RSOC) as well as the Texas cybersecurity incident response team (CIRT) for the Texas Department of Information Resources (DIR). Jeremy and his team respond to incidents, establish play books, coordinate cybersecurity exercises, and perform threat intelligence across the State.

THE INTERVIEWS

Can you summarize for our readers how changes in funding, policy, and priorities are impacting the future of cybersecurity in the public sector?

MIKE WITT - NASA

The external policy and priorities are coming to the agencies in a waterfall effect. I would prefer a more agile approach using a risk-based roadmap. If everything is considered a priority one, government agencies are not staffed accordingly to implement as such. Agencies are scrambling to meet the timeframes established and if they do not have the appropriate expertise, agencies are going to potentially miss the mark on their requirements and architecture designs as well. This ties directly to the funding requirements that we are lacking to implement many of these unfunded mandates.

GERALD CARON - HHS

Among other things, the Executive Order has put an emphasis on Zero Trust. So, it's definitely not just an IT problem, but it is putting the focus at the agency level. I think [the Executive Order] has brought forth prioritization at the agency levels so they understand that this is important, we need to be taking care of this, and it's not just the IT guys doing it themselves. There is also a Technology Modernization Fund, which is a great thing that people are taking advantage of. There's a lot of great working groups, working together to understand commonalities, trying to solve the same problem. In some instances I've seen in the past, not necessarily saying this is done everywhere, but when we have a modernization effort, security has been an afterthought. I'm a big proponent of baking [cybersecurity] in. If you're going to have this Zero Trust architecture, build that security in so it plugs in and it's predictable when it gets deployed into production.

JEREMY WILSON - TEXAS DIR

My agency, DIR, has roughly over 200 people, which is pretty small when you think about delivering statewide security services. Unlike a lot of state agencies, most of our services are cost recovery. There's a fee that's tacked on that funds our programs. We also recently received funding from the legislature, particularly over the last special sessions. There's a lot of interest by elected officials into expanding our various cybersecurity

programs, providing more services, and getting more entities signed up. With that, there were several initiatives that were attached with actual legislative funding for programs.

What is your take on privilege protection strategies as it pertains to a Zero Trust identity security strategy?

MIKE WITT - NASA

I think the strategy is a large part of our future, but there are still maturity gaps in the various zero trust technologies. You need to do your own testing – trust but verify. I am lucky in that I have a very skilled cybersecurity engineering staff who is focused on this.

GERALD CARON - HHS

Privileged users, whether they be administrators, power users of an application, application owners, things like that, they're definitely a hierarchy of the user population. When you look at something like Zero Trust, it's about getting the right data to the right people, at the right time. When it comes to a privileged user, historically, they get their privileges as a result of being part of a group that delegates them that privilege or those accesses. Doing things like just-in-time administration and just-enough administration are very important. Just-in-time administration is time-bounding. When that account is not in use, it's pulled out of that group, so when it's compromised, it doesn't have that elevated access. We've been talking about least privilege for years. We need to have some governance over identities, make sure that they do truly have the correct privileges, and that they only get just enough information when they need it, if they're allowed to have it. These are age old practices, but they really should be applied. I think the technologies are getting better so we can better leverage those kinds of concepts.

JEREMY WILSON - TEXAS DIR

The bad guys are always looking for a way in, so if your data's locked up, your network's buttoned up, and your data center has good security, then the easiest way in is to try and trick a user to click a link or compromise user credentials. If the stolen credentials have privileged identity, then it's much easier for them to move around and gather what they need. So, regular identities need to be secured, hopefully with some kind of multi-factor authentication, and there needs to be robust monitoring around privileged identities as well. Having said that, this is not a snap your finger type thing. Some of these projects can be quite complex. There are different

versions of identities and they touch a lot of different things. Sometimes they're working with legacy custom applications, so there's coding that has to be done, and you need to go through some serious testing before you can move those things into production. It's better to start on that journey and take a risk-based approach, looking at your system administrators and network administrators and asking - "Are they going in [to the network] via a remote desktop? Is there a VPN? Is there some kind of MFA on those systems? Are they being logged?" All those questions are very important and can prevent a successful breach or attack.

> When you look at something like Zero Trust, it's about getting the right data to the right people at the right time."
>
> - Gerald Caron

Privileged accounts are a subset of accounts that provide the highest level of privileges and permissions to perform a task. Why are least privilege access controls important?

MIKE WITT - NASA

Simply put, least privilege enforcement helps to reduce the overall cyber attack surface. You should grant a privilege only to a user or role that absolutely requires the privilege to accomplish necessary work.

GERALD CARON - HHS

Because you want to be judicious, especially when we talk about Zero Trust. At the end of the day, we are trying to protect data. So, if someone is compromised, my first question as a cyber analyst is - "What did they have access to?" That's what I'm concerned about; knowing what people are supposed to have access to as it pertains to their job, knowing when they need it, controlling that, and being very judicious. That's the least privileged aspect, not perpetually having access.

> Simply put, least privilege enforcement helps to reduce the overall cyber attack surface.”
>
> - Mike Witt

Why is it important to keep Privileged Access Management (PAM) as a separate use case/requirement from Identity and Access Management (IAM)?

MIKE WITT - NASA

They work together, but each have a different audience; PAM defines and controls the administrative role of users with privileged access, whereas IAM deals with your everyday users who are accessing business-specific applications and data.

GERALD CARON - HHS

Because of the result of what they potentially have access to. Your privileged users are usually your highest users and they have special access to things in that data that you are trying to protect. When a malicious adversary, whether it’s an insider or an outsider, gets hold of a normal user account, the first thing they try to do is elevate themselves to a more privileged level or account. If your privileged users somehow get hijacked, [malicious actors] can have access to the data that you’re trying to protect. They have the keys to the kingdom, so to speak. So, you need to understand who your privileged users are and have as few as possible, and you want to make sure you have protections and monitoring around those.

JEREMY WILSON - TEXAS DIR

When you think of it like a Venn diagram, they intersect because they’re both identities. Everybody in your organization has a user role that, hopefully, doesn’t have administrative access. In the privileged identity space, there are different tools, strategies, and tactics for how often you want your administration to log in and how challenging it might be.

How does Privileged Access Management fit into the overall objectives of agency modernization?

MIKE WITT - NASA

It's part of CDM/DEFEND phase 2 so that agencies understand "Who is on the Network?" This ensures that your agency will have the appropriate privileged access controls in place.

JEREMY WILSON - TEXAS DIR

When you're talking about modernization, you're trying to shore up all of your defenses and make sure that everything is being tracked and audited, and that you're using the best-in-class practices and tools to prevent unauthorized access. So, to me, [PAM] is just part of an overall approach to strong security across the enterprise.

If least privilege principles are not applied, what are some examples of what adversaries could achieve?

MIKE WITT - NASA

I can provide a real-world example for this question. If you remember the SolarWinds incident, victims unknowingly downloaded a trojanized software update from the vendor. Once installed, the malware connects to external domains as part of its command and control feature to check-in. If your organization did not have the appropriate least privilege security controls in place, your infrastructure was then vulnerable for the next stages of this attack that allowed the adversary to gain a foothold within your network.

GERALD CARON - HHS

If you get an enterprise or a domain admin for Active Directory, you have the keys to the kingdom. If [the malicious actor] gets a tenant administrator for your Office 365, or Azure, AWS, then they own everything in that environment. I've seen bad admin hygiene for a very privileged account many times. I've seen bad passwords, easy passwords, or administrators with 15 different administrator accounts, and they have to remember passwords for all of those things. So, it's very important to understand that you have to practice good admin hygiene, and have the least number of privileged accounts possible, because you can possibly give away the keys to the kingdom if those get compromised.

JEREMY WILSON - TEXAS DIR

So, say I have [privileged access] that I don't really need and my account gets compromised. [The malicious actor] could turn off any security tools I have on in there. They can turn off logging and other things like that. For us on the state government side, the keys to the castle - [Personal Identifiable Information (PII)] citizen data, financial data - would, in most cases, be what they're looking for. If somebody has access that they shouldn't have, you're looking at a wider user base that could potentially have access to the sensitive databases and things of that nature.

Is there anything else you would like to tell our readers about that we haven't yet discussed?

GERALD CARON - HHS

I think identity, especially at the privileged level, is a very important pillar of Zero Trust. Again, Zero Trust is about protecting the data. We can put perimeters around the different types of data, but we have to make sure the right people can access the right data at the right time. So, identity is very important. As we've discussed, your privileged users, if compromised, could possibly be very damaging.

> Security is a journey, not a destination."
>
> - Jeremy Wilson

JEREMY WILSON - TEXAS DIR

I've been fortunate to work on some pretty good security teams and you're never done. So, I always say, "Security is a journey, not a destination." You always have to be looking forward. At some point, organizations need to be serious about investing in security programming, meaning people, resources, and time. I've spent a lot of time talking about low-cost and no-cost initiatives. Even if you don't have a lot of funding, there are still things that can be done to improve your security team. Then when the funding comes, you can decide how to allocate it. As a security team, start finding out from the business what metrics and KPIs matter to them so they can see their return on investment.

MIKE WITT - NASA

Here are some things that I always like to share for others to keep in perspective:

- Know your **organization's risk tolerance**; every federal agency or company is different.
- Make sure you **have business empathy**; compliance is NOT usually the corporate business priority.
- **Implement cybersecurity guard rails** that allow your users to still perform their jobs.
- Embrace automation, orchestration, and zero-trust; it's our future – however, **verify the technology works** as advertised.
- Intrusions, breaches, and malware incidents are going to happen; make sure you **have a plan**, and make sure your team exercises this plan in advance.
- Lastly, **never waste a good crisis**. They can be learning opportunities.

INDUSTRY PERSPECTIVE

JOSH BRODBENT, RVP, PUBLIC SECTOR SOLUTIONS ENGINEERING, BEYONDTRUST

Josh has more than 20 years in IT experience and has architected identity and privileged access management solutions for over 3 million user accounts. He joined BeyondTrust in 2018 as a Senior Solutions Engineer and was quickly selected to lead the team. Prior to BeyondTrust, he was a Senior Solutions Architect for Quest Software. He began his career by founding a managed service provider (MSP) at 12. He held multiple industry certifications by 14, making him the youngest in the nation to do so. That MSP went on to become successful, and ultimately his launching point into Public Sector architecture and support.

INDUSTRY PERSPECTIVE

JOSH BRODBENT, RVP, PUBLIC SECTOR SOLUTIONS ENGINEERING, BEYONDTRUST

In your opinion, how are changes in funding, policy, and priorities impacting the future of cybersecurity in the public sector?

There is much more focus and momentum behind having a strong cybersecurity posture. It's the funding piece that will either make or break the public sector's ability to act on those policies and priorities. As seen with the recent Executive Order from the Biden Administration, there are specific and desired outcomes that the Administration hopes to achieve through cybersecurity. The technology exists to realize those outcomes. The unknown variable is whether or not the budget will exist to acquire and implement the technology.

Why are least privilege access controls essential for public sector cybersecurity?

Simply because the cybersecurity perimeter is no longer a defined line, like the "data center" or "network". The modern cybersecurity perimeter is a concept. It is an intangible perimeter made up of applications, hardware, endpoints, etc., and the interactions between and among them. Without absolute command over privilege access controls, you cannot secure the perimeter.

How can Privileged Access Management fit into the overall objectives of agency modernization?

Agency IT modernization is not a defined policy or set of principles; it is a mindset. One primary objective of this mindset is to establish the most robust security posture possible while, at the same time, enhancing productivity to support mission goals. This objective is achieved when the security of elevated privilege is aligned with speed and efficiency specific to the task at hand.

ABOUT GBC

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive's* 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research analysis.

For more information, email us at research@govexec.com.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

Learn More at: https://www.beyondtrust.com/.