ARTICLE

BeyondTrust

Cyber Leaders Exchange:

Securing Paths to Privilege™

Adversaries seek to gain access to privileged users' credentials to mimic real users. BeyondTrust and Microsoft experts share ways to counter such attacks.

Written by Jory Heckman, October 2024

As federal agencies evolve cybersecurity strategies, more adversaries are exploiting privileged user credentials to gain access to their networks.

And those privileged user credentials are becoming a more attractive target as agencies implement zero trust architectures, pointed out Steve Faehl, chief federal security officer at Microsoft Federal.

"Don't assume that your admins are using your admin credentials. In fact, you should assume that others are using your admin credentials," Faehl said.

"Any sufficiently advanced attacker will be indistinguishable from an insider threat — if you think about the things that your insiders are doing with privilege today and think about what those might look like being weaponized," he added. "Those are all things adversaries absolutely can do and want to do. They want to look just like your users while they do it."

That's why agencies need to understand who has access to these privileged user credentials and to minimize the chance those credentials are exploited, said Michael Saintcross, vice president for federal at BeyondTrust.

"Privilege is everywhere, and we don't have a holistic visibility to that privilege," said Saintcross, who joined Faehl for a panel discussion during Federal News Network's Cyber Leaders Exchange 2024. "At BeyondTrust, we talk about the Paths to Privilege™ — about having visibility, that insight into misconfigurations, and having the ability to make those changes, to automate those — but also respond to threats, to detect them and detect action."

As agencies implement their zero trust strategies, cybersecurity officials are focusing on the identity pillar to reduce the attack surface.

"We're trying to eliminate the most critical attack vector, which is privilege escalation. You have lots of exploitability out there," Saintcross said.

Achieving 'least privilege' with zero trust

Faehl said paths to privilege "are absolutely a place to prioritize when it comes to your investments in protection and remediation."

Remember: Adversaries are opportunistic, Faehl said. "As a result, can you think about that surface area and what your identity strategy is to reduce that surface area for attackers?" In other words, look at how to harden the identities and restrict potential paths to privilege, he recommended.

We can't completely eliminate privilege, but least privilege is a key philosophy behind zero trust. The more defense in depth around identity, the better off federal agencies are going to be," Faehl said.
Saintcross added that more organizations are removing cached privileges across their infrastructures to minimize these types of threats.

"We're going to be eliminating that attack vector," he said. "These common attack vectors, that are still being executed today, they're not being addressed because there isn't that enforcement of privilege execution."

Agencies are also getting more judicious in granting privileged access to their networks. That includes microsegmentation of their systems and offering zero standing privileges that limit user access to the minimum necessary to perform a task.

BeyondTrust

"Privilege is granted at the time of need, and there may be general administration that's one-time, and it can be granted upon request," Saintcross said. "Say somebody needs to have a remote desktop session because they have an application they have to make some administration changes on, and they get that access. They're allowed to do certain commands or use certain application features. Then their session expires, and the privilege is removed."

While agencies must grant some certain level of privilege out of necessity, Faehl said they can reduce their risk by modernizing or getting rid of legacy applications and infrastructure they no longer need.

"In the interest of reducing adversary opportunity, any time that we can reduce that attack surface by eliminating infrastructure, it's a really great play," he said. "And then we can effectively audit and minimize any risk that is the result of privilege identity use as well."

Increased network visibility and managing privilege

As agencies gain more visibility into their networks, they will likely discover more potential cyberthreats. "Along the way, you're going to find quite a bit of vulnerability. You're going to find quite a bit of threat," Faehl said. "You're going to find assets you didn't know you had. You're going to find users you didn't know you had. You're going to find lots of usage that you didn't know you had. And so, it can actually be quite a shock for organizations that are undergoing a zero trust transformation. It's definitely not business as usual, and you're going to see many more threats," He added: "It's not that you are worse than you were before. It's that before you were 'watermelon green' — you were green on the outside, red on the inside."

Although agencies may experience shock at the number of potential threats out there, Faehl said having that threat visibility is a critical step to minimizing risk.

"If you don't have the visibility — if you don't have the telemetry, if you don't have the metrics, you don't have the auditing, you don't have the analytics to run on top of it to really rationalize the context of that data — you can't know if you're green or not," he explained. "Sometimes, maturity looks like one step back, in order to take three steps forward, but it's not really a step back. Knowing the truth about your environment is never a step back. And so, I think that's a huge mindset shift that needs to take place, and I see many agencies embracing it."

Adopting AI/ML cyber tools

To stay on top of the growing volume of cyberthreats, agencies are turning to artificial intelligence and machine learning tools to automate threat detection.

"We've had a lot of detections that have increasing efficacy. We have scenarios now where we're able to feed environmental telemetry to say, 'Your organization, is under attack, therefore pivot your models, pivot your response. Have adaptive security that changes based on those threat conditions for your particular environment,'" Faehl said.

Saintcross said that level of automation is becoming necessary to keep up with "needle in a haystack" scenarios and to analyze huge volumes of data to identify suspicious behavior.

"Humans can't keep up with the data volume, the alerts, or even just the task of building new models to find that suspicious behavior," Saintcross said.

"Fusing that data together is where we're able to identify the misconfigurations, access attempts, or abnormal behaviors as suspicious," he added.