How to Keep Your Bearings in Today's Threat Landscape

Government has been driving toward zero trust-based cybersecurity methodologies for the past couple years. The bad actors know this. That begs the question: What are the most pressing threats that continue to challenge that methodology?

In a recent digital GovLoop event, experts from government and industry discussed the current threat landscape, and offered guidance to help shape the cyber agenda for 2024.

The Speakers

- **Beau Houser**, Chief Information Security Officer, U.S. Census Bureau
- **Jason Zann**, Office of the Federal Security CTO, Microsoft

The Threat Landscape: Persistence Pays Off

Bad actors know that government is pivoting toward zero trust, and they are adapting their attack strategies accordingly, both by adding to their arsenal and focusing on proven tactics. Key threats include:

Phishing, Phishing and More Phishing

Despite all the effort that's gone into training people not to click on suspect links, "we're still talking about phishing," said Beau Houser with the U.S. Census Bureau. "The reason it persists is because it works. The cybercriminal groups are able to make money and advance their objectives."

Even with zero-trust strategies in play, "there's no such thing as perfect protection," he said. With phishing scams targeting people's emotional reactions, "it's a people problem as much as it is a technology problem."

"We're still talking about phishing. The reason it persists is because it works."

- Beau Houser, U.S. Census Bureau

Insiders and Pseudo-Insiders

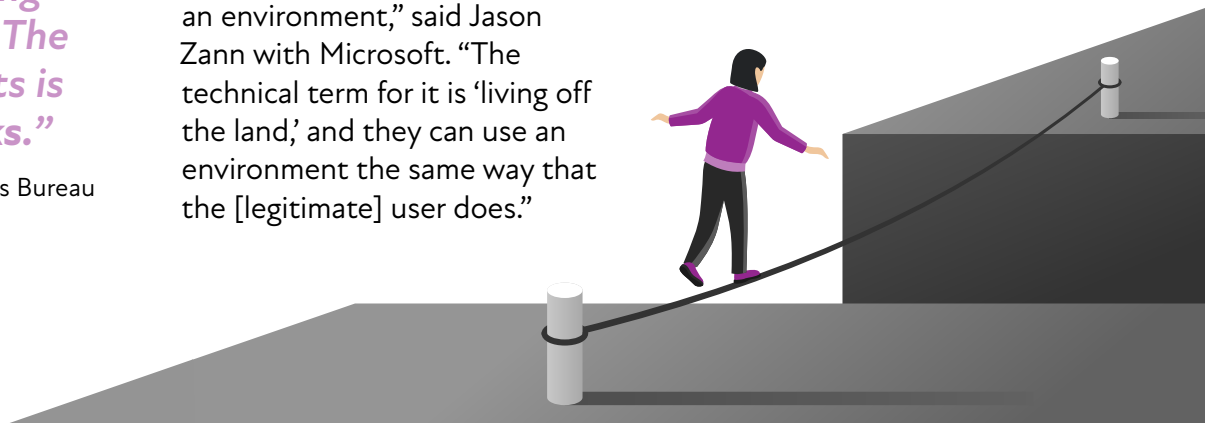
Insiders who seek to compromise data or systems can cause "tremendous damage," Houser said. "You need extra capabilities when you're dealing with those intentional insiders, those malicious insiders. It all comes down to knowing what's happening on your network, and then being able to determine what's not right."

It's worth noting that this attack vector applies to not just the actual insiders, but also those who pose as insiders. In some cases, "an adversary has the ability to assume the roles and responsibilities that the federal user has within an environment," said Jason Zann with Microsoft. "The technical term for it is 'living off the land,' and they can use an environment the same way that the [legitimate] user does."

Nation-States

Among those looking to compromise government systems, "the most sophisticated" are the nation-state adversaries, Houser said. "They're very determined, very well-funded and they have a lot of time. They can really curate their attacks over time."

Nation-state adversaries "have larger and larger stakes at play," giving them a powerful incentive to circumvent emerging zero-trust constraints, Zann said. Every move "comes with a different counter-move on the other side. There is a constant tension that continues to evolve over time," he said.



The Evolving Cyber Agenda

Faced with these threats, government IT teams and cyber defenders will need to continue their proactive efforts to stay one step ahead. Here are some steps they can take:

Look beyond identity.

Identity has been key to cyber defense as zero-trust strategies emerge. Knowing who's on the network and what they're allowed to do there is a chief safeguard. "That identity pillar, I think, is really mature," Houser said. Now defenders need to look beyond identity. "We're going to see continued progress in the other pillars: the data pillar, the application tiers," he said.

Defenders need to get to the point where they can say, "Not only do I know the person, through strong identity. I know the device that the person's using, and I expect them to use a known device," he said. "Associating the user with a device really dials up the security quite a bit. Then you can bring in other attributes as well, like geographic location."

Adopt phishing-resistant MFA.

Agencies already are looking to multifactor authentication (MFA) as a foundational piece of zero trust. They can take that further, Houser said, by implementing MFA with an eye toward thwarting phishing attacks.

With phishing-resistant multifactor, "you get to add a lot more attributes to the authorization process than simply the login process," he said. Attackers look for seams in the defenses — misconfigurations they can exploit — and more targeted MFA can help close those gaps. Phishing-resistant MFA offers "an example of how we're adjusting based on what the threats are," Zann said.

Take advantage of AI.

Artificial intelligence (AI) has upended much of the IT world in the past year, and promises to have a big impact on the way security teams leverage zero trust to counter attackers. "The future of AI is very exciting, especially in the short to medium term," Zann said.

"AI has proven itself to be very good at things that humans are not very good at: mundane, repetitive tasks," he said. As analysts sift through masses of cyber alerts, AI can "provide that augmentation to be able to not only lift those signals up, but even to recommend the courses of action that could be taken as a result."

Going forward, "AI will be able to help defenders tremendously ... in separating the wheat from the chaff," Hauser said.

Shift to a community defense model.

The good news: Defenders are not alone. There's a strong community of practice at your back, Zann said.

Community defense refers generally to "how we're thinking about the problem, how we're working with each other to solve common problems," he said.

"There's something to be said about holding your peers, your teams, your vendors, your partners accountable," he said. "If we all address this together, we all stand a chance together."

To learn more, watch the on-demand version of the full event.

"There's something to be said about holding your peers, your teams, your vendors, your partners accountable. If we all address this together, we all stand a chance together."

- Jason Zann, Microsoft

govloop Microsoft