FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES:

Zero trust architecture

Sponsored by TANIUM

TANIUM

Ready for zero trust

Take bold steps to modernize national cybersecurity efforts with new strategies.

To learn more please visit **federal.tanium.com**

How to build a flexible and dynamic zero trust network

BY TOM TEMIN

Federal agencies, seeking both compliance with a White House executive order and better cybersecurity in reality, are rapidly adopting the zero trust model for controlling access to their networks. They're learning that zero trust, like a cake, has many elements that, once combined, are difficult to separate. Zero trust is often described as a mindset. It is. But it's also a set of technical strategies, products and procedures. A mindset is difficult to quantify, but zero trust requires work and investment.

Sanjay Gupta, the chief technology officer of the Small Business Administration, said, "Zero trust architecture is a concept. It's a strategy. It's a mindset. It's a fundamental shift in the way you look at cybersecurity. And so there are many aspects of it."

Fundamentally, Gupta said, zero trust supersedes the perimeter security model.

Zero trust "flips [the perimeter model] on the head to say, you have to protect each and everything inside your environment. Each asset – data, applications, devices – needs to be protected in of itself. And nothing can be trusted inherently," Gupta said.

That's as opposed to the assumption that a perimeter-based firewall will protect everything behind it.

Gupta spoke on a panel discussion among expert federal and industry cybersecurity practitioners, convened by Federal News Network. The purpose was to explore the practical realities of achieving zero trust.

All-encompassing approach

Zero trust can also be a unifying approach to the emerging hybrid model of computing so many agencies have adopted, Gupta said. "It transcends the on-premises computing model, the cloud computing model, the mobile computing model."

Rob Hankinson, the director of information technology infrastructure at the State Department, underscored that point.

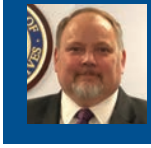
"We certainly have to take into account the cloud," Hankinson said. "We have to take in the on-premise solutions that were developed at our 270 posts overseas. We have to take our various data center applications and pull them in as well."

PANEL OF EXPERTS

Sanjay Gupta, Chief Technology Officer, Small Business Administration

Matthew Marsden, Vice President of Technical Account Management – Public Sector, Tanium

Rob Hankinson, Director of Information Technology Infrastructure, Department of State



Randy Vickers, Chief Information Security Officer, House of Representatives

Hankinson said that State has already acquired many of the technology components for zero trust. But they require reconfiguring, and in some cases, operating in dual modes. He said the staff is in the midst of a comprehensive planning phase, mapping its IT assets against the cybersecurity control outlined in NIST Special Publication 800-53 and against the Defense Department's zero trust roadmap.

"So we're doing that gap analysis," Hankinson said. "We're also doing it with our common control providers, our identity providers, our data providers, also walking them through this to build that solutions architecture."

The architecture in turn will enable the IT staff "to see what we have, what we need to procure, what funding we need to go after and when we need to go after that," he added.

Among the foundational elements in a zero trust architecture: identity management. That's the starting point for the House of Representatives, according to Randy Vickers, its chief information security officer.

"You've got to have the immutable person," Vickers said.

An individual with a given set of permissions can change roles, or leave and return, and therefore acquire a different set of resources he or she may access.

"But you've got to start with identity. Identity validation, as someone provisions into the environment, is key and critical," he said.

Vickers said his staff is building out a public-key infrastructure system, to bring encryption in as a way to secure identities and access.

For effective zero trust, the single trusted identity for each individual – or robotic process, for that matter – must apply across the silos of technology.

"The idea here," Gupta said, "is you have to break those silos down and get to an enterprise level of looking at things like an identity solution, as opposed to having multiple identity solutions in your environment."

End user view

When agencies like the State Department operate throughout the world, geolocation services come into play for zero trust. Sometimes users operating outside of the continental U.S., Hankinson pointed out, need different devices than when they're operating in the continental United States. Similarly, Vickers said House members and staff regularly travel overseas, something the zero trust implementation must take into account.

The considerations can be complex, and require challenge-response mechanisms down to the data set level.

"As you're looking at data sets, that roadmap to get one data set to zero trust might be fundamentally different than for a data set sitting right next to it, or sitting it somewhere else in the organization," Hankinson said.

The expansion of telework with the United States and the wider adoption of bring-your-own-device policies has added another complication to implementing zero trust.

Matthew Marsden, the vice president of technical account management at Tanium, said it implies a need to invest "in workforce, culture and mindset, getting the people using the systems to understand the premise of least privilege and moving away from the traditional 'badge-in and have access to everything' mindset."

Beyond verifiable identities, zero trust requires continuous assessment and authorization, both of the user identity and of the device with which the user logs in.

That process has three basic components. First, verifying the user. Second, permitting log-in with multi-factor authentication, ideally under a security assertion markup language (SAML), system. And third, verifying the device.

That last item, verifying the device, requires distinguishing whether the smart phone or remote PC is government-furnished or private.

"Then you need to be able to dynamically assign policies based on those two factors," Marsden said.

A trusted user on a known – say, government-issued – device will get one response, whereas a trusted user on an unknown or untrusted device will get another. In the second case, some data might be rendered off limits.

Marsden added, "As user and device requirements change, new vulnerabilities appear on the network, and device posture changes, you need to be able to continually assess authorization and access, and apply policies as needed, on the fly."

Federal agencies, given their size, numbers of users, and range of data they deal with, must, therefore, deal with exponentially more variables than can be monitored manually.

"The implication," Gupta said, "is heavy automation, use of tools like machine learning and artificial intelligence. You basically think of it as, you put all that information in through a dynamic engine, which at the spur of the moment decides, and says what level of access this individual will have at that given moment."

Who owns the device?

He said SBA revised its policy under which only government-furnished equipment could access applications and data. In fact, he said, "We broke that."

Why? Simply because at the outset of the pandemic, when Congress gave the agency responsibility for disbursing hundreds of billions of dollars in relief dollars, SBA didn't have enough gear to furnish all of the people it had to hire.

"The need of the hour was to have our staff productive, and there weren't enough laptops available," he said.

The solution was what Gupta called conditional access, within a risk management framework, that let people get around traditional restrictions.

A process known as device interrogation comes into play here. Interrogation leads to verification, if appropriate, and authorization. Interrogation informs the presumably automated authorization process whether the device is patched, is configured according to policy, and whether the user is employing an approved authentication request mechanism. All, Marsden said "so you can make an informed decision about whether an authenticated user can still access the network on the device that they're using. Then you have to apply the appropriate dynamic policies" for what privileges and permissions the user and device will have.

Ultimately, a zero trust architecture, panelists agreed, must operate under an agency's risk management framework. Applications and databases need not all be treated the same, because sensitivities vary.

"Do I really need all these different checks, if all I'm doing is going to a publicly accessible something? The answer is no," Vickers said. "But to go to this other thing, I need these checks that the user may yell and scream about. What risk are we trying to mitigate? What risk posture are we trying to maintain or change? That's the key."

Zero trust is now the goal of policy in an environment where users employ everything from trusted devices on classified networks to employee-owned smart phones working from a public WiFi location. Therefore no two solutions will look alike.

"If there is an expectation that there is a cookie cutter answer to zero trust implementation," Gupta said, "there isn't one, and there should not be an expectation that each and every implementation of zero trust will be identical."

On the other hand, each agency need not start from scratch. Said Vickers, "We all learn from other people's implementations, and use the pieces, parts, frameworks and standards that we can make applicable to ours."