FEDInsider

Federal Agencies Are Building A Zero Trust Framework Component by Component

As IT leaders in government prepare for federal cyber mandates, they're already implementing data strategies and identity management fit for zero trust architectures.

Featuring:

- **Robert Wood**
  CISO & Director, Information Security & Privacy Group, Centers for Medicare & Medicaid Services

- **Randy Resnick**
  Director, Zero Trust Portfolio Management Office, DoD

- **Ida Mix**
  Chief Information Security Network Officer, Bureau of Industry & Security, Department of Commerce

- **Kevin Hansen**
  Chief Technology Officer, Public Sector, MFGS

The White House's 2021 Cybersecurity Executive Order is moving the government towards a zero trust architecture approach to protect federal data. To help agencies adopt best security practices and advance these efforts, government and industry are working together to migrate to a zero trust architecture in the most effective way.

Government and contracting community security experts spoke at a recent FedInsider roundtable about their experiences with adopting zero trust, multifactor authentication and identity management to determine access and bolster cyber hygiene. The following are some of the most important aspects of their discussion.

Zero Trust as a Framework and Strategy

Adopting a zero trust architecture isn't a one-time purchase. It's a cybersecurity framework and strategy that comes in components that enable zero trust capabilities, said Randy Resnick, senior advisor in the Zero Trust Portfolio Management Office within the Department of Defense's Chief Information Office/Cybersecurity.

"When you are implementing zero trust, what you are doing is saying you're going to have a user inventory of exactly who is allowed to get on your network, as well as the devices that are allowed to get on the network, which include mobile devices," Resnick says.

Each user and device must pass two tests to get into the network – they must be authorized and authenticated. Then, there are further tests depending on the user or device requesting access to data, applications or resources. These rules are set in privileged capabilities or policy points within the architecture – in the Identity, Credential and Access Management framework. ICAM allows system owners to have assurance that the right person is accessing the right data.

From a commercial standpoint, helping agencies adopt zero trust capabilities requires aligning to customer priorities and desired outcomes. Kevin Hansen, chief technology officer for public sector at Micro Focus Government Solutions, says that entails providing application security, identity and access management, data management and protection, and embedded analytics for cybersecurity operations.

"Our broad portfolio and alignment across multiple zero trust pillars really allows us to help address the needs and priorities," Hansen says. "But we're also helping to focus on the interoperability and advanced maturity of the programs."

Overcoming Common Zero Trust Adoption Challenges

Federal agencies are facing adoption hurdles when it comes to zero trust, like limited resources, legacy systems and tight timelines. For Ida Mix, chief information security network officer in the Bureau of Industry and Security at the Department of Commerce, one of the biggest challenges is coming up with solutions that work within their existing budget. Smaller agencies typically get less funding, but that doesn't mean Mix isn't still asking for the resources they need. But it may require having to justify the need for the extra funding.

"That's where the security gap analysis has helped us," Mix says. "It identified certain things that we needed to do." Plus, the department adopted a shift left security approach which guarantees application security at the earliest stages in the development lifecycle. That helped to prove the

need for the extra funding required to begin the move towards zero trust, which allowed the security team to begin to secure their network.

For the DOD, Resnick says the department is making sure its zero trust architecture is interoperable enterprise wide, and rules are translatable as devices change and advance. "As you implement your solutions, you constantly ask for interoperability. You absolutely don't go proprietary when it comes to protocols, no matter what the vendor says," Resnick says. One-off solutions can create communication disconnects from the enterprise solution, which could also disrupt zero trust security practices.

Zero Trust and Data Protection

Data is a critical component of any zero trust architecture. Hansen says that it's so important that it requires setting up various policies regarding both the value of data and the risk of access to it. "Those two variables may, for example, drive a different security policy for a high value piece of data compared with a less valuable one," he says.

He referred to the federal data strategy as a resource for data management in government as it relates to zero trust, and protecting data against theft and misuse. Data must first be discovered, analyzed and categorized correctly so that proper protection policies can be determined. Then, data can be monitored, archived and managed.

Once the lifecycle of data is managed, "as it relates to zero trust, being able to change the policy based on the risk associated with the access is where that becomes really important," Hansen added.

The Department of Commerce is taking a granular approach to data access. Mix says they implemented a compartmentalized architecture, using VPN zones on the network, which requires every VPN zone to go through the firewall. This way, no device on the network can communicate directly with another device on the network. A user must go through a switch or the firewall. This helps to prevent a bad actor gaining access to all data on the network even if there's a breach.

Critical Access and Identity Components to Zero Trust

Multi-factor authentication pre-dates federal zero trust mandates, but is essential to achieving a well-rounded zero trust architecture. Hansen says it is the best mitigation against a large majority of attacks as it limits lateral movement across networks, and may be one of the best starting points for zero trust.

In fact, multi-factor authentication's continuous authentication and authorization process can be improved in a zero trust environment by having a centralized framework. This way, applications can hand continuous authorization and authentication off to a centralized enterprise service that supports all multi-factor authentication factors, ensuring in a zero trust architecture that all are accounted for with the appropriate risk-based access policies.

Identity management is also a critical component to zero trust, and the Centers for Medicare & Medicaid Services is looking to strengthen security in this area. Robert Wood, chief information security officer and director of the Information Security and Privacy Group for CMS, says the agency has a team that manages identities and authorization for external constituents, or consumers of applications, and internal federal contractor team members.

"We're doing a lot to basically build security controls into that technology, so that they can be inherited," Wood says. For example, app-specific security policies for federated logins are inherited from and by the users and applications that are working there. CMS is also looking into machine and service identity by building out a platform-as-a-service environment that will authorize and authenticate every service-to-service interaction.

Considering zero trust is a framework that comes in components that will shift and evolve over time, agencies are adopting the ones that, together, will help prevent and contain security issues when they occur.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

- (202) 237-0300
- Info@FedInsider.com
- FedInsider.com
- Facebook.com/FedInsiderNews
- Linkedin.com/company/FedInsider
- @FedInsider

carahsoft.

Carahsoft
14993 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Aowab Alwazir**

- (703) 921-4165
- Aowab.Alwazir@Carahsoft.com
- Carahsoft.com/microfocusgov
- Facebook.com/Carahsoft
- Linkedin.com/company/Carahsoft
- @Carahsoft