DARKReading

Federal CIOs Zero In on Zero Trust

10/16/2019
William Peteroy

https://www.darkreading.com/endpoint/federal-cios-zero-in-on-zero-trust/a/d-id/1336038

Here's how federal CIOs can begin utilizing the security concept and avoid predictable obstacles.

Now more than ever, the US government has focused on proactive cybersecurity measures. Under President Donald Trump's proposed budget for fiscal year 2020, the federal cybersecurity budget would increase to $17.4 billion, up from an estimated $16.6 billion this year.

The budget increase shouldn't come as a surprise, as major data breaches continue to cripple organizations of all sizes and sectors worldwide while malicious nation-state adversaries continue to apply pressure, especially on government organizations. With cybercrime continuing its steep trajectory, it's projected to cost the world $6 trillion annually in damages by 2021, according to Cybersecurity Ventures.

Within cybersecurity spending, one of the areas federal CIOs are eyeing is the concept of zero trust, due in part to recent reports from the Defense Innovation Board and the American Council for Technology-Industry Advisory Council. Zero trust is now front and center for federal CIOs, but where exactly should they begin?

Beyond Jargon: What Is Zero Trust?

Zero trust fundamentally focuses on establishing new perimeters around sensitive and critical data. These perimeters include traditional prevention technology such as network firewalls and network access controls, as well as authentication, logging, and controls at the identity, application, and data layers.

While the concept sounds simple, especially as information security vendors claim to make the road to zero trust easy with their products, the reality is much more complex. Zero-trust architectures (ZTAs) require extensive foundational investments and capabilities as well as extensive logging and control layers that are largely in the traditional IT stack more than a plug-and-play security technology.

Getting Started

Federal IT environments are complicated, and as CIOs take a closer look, they will see in many cases they're already notionally on a path to Zero Trust. There are a number of foundational requirements that are not unique to Zero Trust that map back to the DHS's Continuous Diagnostics and Mitigation (CDM) program.

To get started on the road to zero trust, government organizations should begin with CDM Phase 1 requirements that focus on understanding what's on the network. The CDM Phase 1 requirements include:

- Automation of hardware asset management
- Automation of software asset management
- Automation of configuration settings
- Common vulnerability management capabilities

By following these requirements, federal CIOs can begin to gain a true understanding of the sheer amount and sensitivity of the data they hold.

The Obstacles in the Road

ZTA generally assumes that an enterprise has fully embraced concepts such as DevOps and has limited legacy data and applications. Federal networks are different because they have been around longer and have more legacy technology than most enterprises. They also leverage secure facilities for access to sensitive data and are already under constant attack from nation-state adversaries.

Beyond CDM Phase 1 requirements, federal CIOs should shift focus to identifying critical data in their networks and building secure applications and identity management systems around that critical data. Once sensitive data has been identified, network and application logs should be used to determine who accesses the data on a regular basis; this information can be entered into traditional network-layer and application-layer controls, such as firewalls and role-based access to applications and data.

Today, one of the biggest decisions that federal CIOs must make is how they shift their development requirements for current, next-generation and legacy applications. With the advent of ZTA, it's likely that CIOs require all applications to use a centralized identity, credential, and access management solution. But when it comes to current applications, there is a significant cost to retrofit access controls (adding firewalls and application gateways) and it's unclear who will foot the bill between security: IT or application development teams.

The final challenge will be around legacy applications such as mainframe applications, which are common in data-intensive government lines of business applications. Without a straightforward way to add layers of protection and monitoring to these systems, CIOs will either spend money to completely redesign these systems or accept that a true ZTA is still beyond their reach or the reach of their budgets.