WHITEPAPER — ZERO-TRUST ARCHITECTURE

A Security Strategy Whose Time Has Come

Jeanne Zepp

INTRODUCTION

In May 2021, President Biden issued Executive Order 14028 seeking to improve the cybersecurity status of the United States. The directive explicitly stated that a government–private sector partnership is critical to protect federal agencies, organizations and individuals from malicious cyber actors.

The president noted the need for bold federal action and significant investment, as cybersecurity is a prerequisite to national and economic security. A comprehensive list of implementing actions and responsible parties followed.

Modernization of the government's approach to cybersecurity by implementing Zero Trust Architecture both in agency networks and cloud technology is a noteworthy aspect of EO 14028. So, too, is the governmentwide prescription to implement phishing-resistant multifactor authentication (MFA) and data encryption.

The executive order defines Zero Trust Architecture (ZTA) as: "a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries." This definition recognizes that perimeter-based system defenses are outmoded and undependable.

Office of Management and Budget Memorandum 22-09 (OMB M-22-09) takes EO 14028 one step further by outlining a strategy for agency migration to a Zero Trust Architecture. It establishes an implementation deadline of September 30, 2024 for specific goals and objectives.

ZERO TRUST ARCHITECTURE EXPLAINED

Foundational to the concept of Zero Trust is placing no trust in any user or any element of the IT infrastructure. In addition, Zero Trust operates from the premise that unauthorized access is inevitable, perhaps having already occurred. OMB M-22-09 bluntly states, "… no actor, system network or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."

Zero Trust Architecture features ongoing verification of access needs and strict adherence to the least privilege principle wherein users only possess access to the minimum resources needed for job performance. These provisions seek to offer protection against phishing attacks and isolate the impact of successful breaches to specific segmented areas. In fact, the Zero Trust model suggests taking a security posture where agencies consider every application is accessible by the public internet.

Zero Trust Architecture also takes a broader view beyond MFA. OMB M-22-09 recognizes the need for "stronger enterprise identity access controls" and prescribes identity system consolidation in order to achieve uniform identity authentication.

Given that EO 14028 also specified data encryption (both data at rest and in transit), ZTA focuses on the Domain Network System (DNS) protocol and the Hypertext Transfer Protocol (HTTP) as well as email.

ZERO TRUST SECURITY GOALS

Relying on the expertise of the Cybersecurity and Infrastructure Agency (CISA), governmentwide Zero Trust goals align with CISA's five pillars: Identity, Devices, Networks, Applications and Workloads, and Data.

Identity

Government agencies moving toward Zero Trust will require personnel to use "enterprise-managed identities." Moreover, OMB prescribes MFA technology that is resistant to phishing attacks.

Regarding the former, identities must be tied to individual job responsibilities/authorities with identity verification occurring at the time of each log-on. These dimensions are foundational to establishing risk-based access. So, too, is collecting and storing metadata about users. Promoting enterprise-managed identities and consolidating identity authentication systems seek to achieve two goals: (1) decrease the labor-intensive effort of agency staff managing credentials and (2) better identify inappropriate activity through enhanced insight into user actions.

OMB M-22-09 establishes that MFA integration should occur at the application level (not at the underlying network level). Recognizing there are different approaches to MFA, OMB further specifies that federal agencies must employ phishing-resistant MFA. It suggests applying the federal Personal Identity Verification (PIV) standard or the Web Authentication (WebAuthn) standard promulgated by the World Wide Web Consortium. OMB points to the use of phishing-resistant tokens, including the PIV cards that contractors and federal employees already possess.

Authorization, separate and apart from authentication, gains prominence in Zero Trust Architecture. OMB defines it as "the process of granting an authenticated entity access to resources." Simply put, authentication verifies a user's identity whereas authorization addresses whether that user is permitted system access. Ideally, each operates using different controls. OMB suggests attribute-based access control (ABAC) in combination with role-based access control (RBAC), specifying authorization systems should include one device-level signal in addition to identity information for the authenticated user.

Devices

Inventorying and cataloging devices used for official business is fundamental to ZTA implementation. So, too, is endpoint detection and response (EDR). CISA plays important roles in both tasks. Regarding asset inventory, federal civilian agencies must participate in CISA's Continuous Diagnostics and Mitigation (CDM) program per EO 14028 in order to better detect and monitor assets. Further, the EDR tools that agencies employ must comply with CISA's technical specifications. Agencies are encouraged to engage with CISA to identify coverage gaps, among other issues.

Networks

EO 14028 specifies that agencies move toward encrypted DNS queries and HTTP traffic, encrypted email, network segmentation and local microsegmentation. Agencies must develop and obtain approval of a ZTA plan addressing segmentation and microsegmentation.

Regarding encryption, the importance of network monitoring versus the susceptibility of devices associated with this activity is a concern. Use of the Transport Layer Security (TLS) protocol is recommended due to its ability to thwart bulk decryption. OMB recognizes there are challenges related to encrypting DNS and HTTP traffic as well as email. Regarding the former, OMB encourages agencies to collaborate with CISA and adopt standards that move them closer to ZTA in terms of DNS requests and implementation of HTTPS, even for internal traffic. As to the latter, encrypted email is not ready for short-term implementation, but an issue CISA and OMB will seek to solve jointly.

Applications and Workloads

The government takes the stance that no user, system or system element is trustworthy. Thus, everything must be verified, and all applications must be viewed as connected to the public internet even if they are not. In this environment, security testing gains prominence, independent third-party assessments become essential, and public vulnerability reports assume a valued role. Just like devices, a complete inventory of applications is paramount.

Ultimately, the goal in ZTA is to make applications internet-accessible but to do so safely. Agencies are required to select one FISMA Moderate system that is not accessible via the internet and bring it online in a way that is secure and fully operational. Doing so assures that agencies can implement the requisite monitoring and security requirements including denial of service protections, access control and an enterprise identity management system.

Regarding workloads, OMB M-22-09 champions immutability due to its contributions to better security. Further, OMB highlights "automated, immutable deployments" as contributing to the objectives of ZTA by "allowing substantially improved least privilege architectures."

Data

Insofar as data and Zero Trust are concerned, agencies must go beyond the protection of datasets and consider "dispersed data systems" and "intermediate datasets" that help maintain primary datasets. The inherent challenge in so doing underlies the decision to form a working group to formulate a data security guide that agencies can follow.

OMB sees a need to automate security monitoring and enforcement, preferring methods based on machine learning. It also anticipates the need to rely on cloud security tools in implementing ZTA, especially key management tools, audit logs and other event data.

ACHIEVING A ZERO TRUST ARCHITECTURE

While EO 14028 and OMB M-22-09 provide discrete goals, tasks and deadlines, risk analysis and management can be a foreign concept to many agencies and their personnel. Toward this end, the National Institute of Standards and Technology (NIST) published a cybersecurity whitepaper (NIST CSWP 20) titled "Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators." It explains NIST's Risk Management Framework (RMF) and delineates how enterprise administrators, system operators and IT security officers can use this framework to develop and implement ZTA. The whitepaper posits there is no one architecture that extends to every agency. Instead, workflow and workflow-related resources, coupled with strategic thinking, will dictate the final form of the agency-specific ZTA.

While each ZTA will be unique to each agency, NIST asserts that common tenets underlie Zero Trust. Such principles pertain to network identity governance, endpoints and data flows. Readers are encouraged to consult NIST CSWP 20 for a full discussion.

The Approach

NIST's RMF is a seven-step process, fully detailed in NIST Special Publication (SP) 800-37, Revision 2. A brief description of each step follows.

1. Prepare – Take a full inventory of enterprise resources, network identities and roles/privileges as well as workflows (business processes) and systems.

2. Categorize – Classify resources as either Low, Moderate or High relative to workflow confidentiality, integrity and availability requirements.
3. Select – Use baseline controls for each categorization (NIST SP 800-53B) and add/delete controls based on "risk to the resource, its known attack surface and its position in the workflow."
4. Implement – Install the controls, emphasizing automation as a preferred means of responding to security changes.
5. Assess – Evaluate the adequacy of controls (system level and process level) amidst a continuously changing environment.
6. Authorize – Place the system/workflow in operation.
7. Monitor – Track activity and enterprise resources, mindful of new threats and potential preemptive measures.

NIST's whitepaper adds an eighth consideration -- using RMF operational loops – in recognition of Zero Trust's dynamic nature.

CONCLUSION

Technology is integral to the operations of the U.S. government. Any activity that impacts technology performance and interrupts mission accomplishment is unacceptable. As the United States moves aggressively toward modernizing its IT infrastructure, it also must modernize its approach to securing this technology from malicious cyberattacks. A Zero Trust Architecture is a critical component of a modern cybersecurity approach.

Zero Trust Architecture is a conceptual framework wherein the end goal is information system access decisions that correctly enforce authorization, identity authentication and least privilege principles in every access request. As a security strategy, it will not culminate in a single solution to be implemented governmentwide. Rather, each agency, reflective of its unique mission, systems and resources, will need to develop controls, tools and safeguards responsive to the risks associated with its mission and the systems and resources that support it. Still, certain methods, such as phishing-resistant MFA, will be important. In addition, encryption, segmentation and microsegmentation will gain prominence.

The challenges are real in moving to a ZTA, however, they must be met and overcome. But, as EO 14028 asserts, the federal government stands ready to "bring the scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises or hybrid." The bold actions captured in the implementing documents articulate a well-reasoned strategy.