Meet the Challenge of Achieving Zero Trust

The zero-trust journey demands a phased, iterative approach.

BY SARBARI GUPTA

NOV 15, 2022

The premise underlying the zero-trust (ZT) security model is simple: All entities requesting access to organizational information technology (IT) resources are assumed to be untrustworthy and their devices and communication networks are likewise untrusted. Within this model, every requesting entity must be authenticated, the security status of every device confirmed, all access privileges verified, and communication sessions with that entity protected (i.e., encrypted) for every access request and every interaction. In addition, the decision to permit access to a resource must be performed as close to the target resource as possible.

Office of Management and Budget Memorandum M-22-09 presents vision statements for each of the five pillars of zero trust: identity, devices, networks, applications and workloads, and data. In addition, the

memorandum offers specific actions (ZT actions) and associated subactions to achieve each vision. Some actions and subactions can be implemented today using available technology solutions. Others will require future technology solutions and/or governmentwide governance approaches. Achieving zero-trust functional goals is no easy task. It requires multiple technology solutions, products and programs. Moreover, the magnitude, complexity and multidimensional nature of the zero-trust journey demands a phased, piloted and iterative approach wherein agencies can take incremental steps to achieve measurable progress.

National Institute of Standards and Technology (NIST) Special Publication 800-207 and NIST Cybersecurity White Paper 20 recommend an optimal first step in moving to a zero-trust environment: Conduct an inventory of current IT resources, end entities and business processes. Why? Because such an effort will help agencies identify and prioritize the risks, they can address through zero-trust principles and, more specifically, the M-22-09 ZT actions.

Based on this risk analysis, agencies can then prepare a Zero-Trust Architecture (ZTA) Strategic Roadmap, offering a phased approach to implementing M-22-09 ZT actions. The road map will be shaped by multiple drivers and strategies such as:

- Agency mission priorities and budgets
- ZT actions that can mitigate the highest cybersecurity risks across the agency
- ZT actions that can improve protection of the most critical resources within the agency
- Other ongoing or planned agency-wide initiatives that can impact progress on ZT actions
- Government mandates that establish target deadlines for ZT action implementation

Once developed, the specific ZTA actions scheduled for near-term implementation within the ZTA Strategic Roadmap need to be assigned to an appropriate agency leader and team. Next, a ZT Action Implementation Plan needs to be defined and leveraged for each ZTA action considering the following aspects:

- The current implementation status of the ZT action, including products and solutions already in use

- Gaps and weaknesses that inhibit full implementation of the ZT action and related sub-actions
- Implementation priority of new/improved ZT functionalities that address the ZT action and sub-actions
- Objectives and target requirements for each new/improved ZT functionality
- Pilot projects that will vet each new/improved ZT functionality and gauge it against specific success metrics
- Implementation of select pilots and documentation of the associated findings and lessons learned
- Quarterly review and update of the ZT Action Implementation Plan to leverage the findings and lessons learned
- Development of a plan to roll out new/improved functionalities across the agency and related success metrics
- Implementation of new ZT functionalities and monitoring progress against metrics
- Iterations on the steps above

Implementing zero trust is a journey that incorporates multiple pillars, actions and subactions, each of which will help strengthen an agency's security posture. Agencies may find themselves paralyzed by the magnitude of the zero-trust journey, realizing that the effort will impact almost every aspect of their operations including policies, business processes, internal and external stakeholders, and, of course, the entirety of their IT environment. Yet, adopting the phased, iterative approach described above will break down this complex, multiyear journey into manageable steps that build upon one another and demonstrate measurable progress along the way.

Sarbari Gupta is the CEO of Electrosoft Inc., and a member of AFCEA's Zero Trust Strategies Subcommittee under the AFCEA Cyber Committee. She received M.S. and Ph.D. degrees in Electrical Engineering from the University of Maryland, College Park and a B.Tech. degree in Electronics and Electrical Communication Engineering from the Indian Institute of Technology, Kharagpur.

For more on zero trust, be sure to check out the December issue of SIGNAL *Magazine.*