CISA Publishes New Guidance for Achieving Zero Trust Maturity

The US Cybersecurity and Infrastructure Security Agency (CISA) this week released the second version of its guidance for achieving zero trust maturity.

The Zero Trust Maturity Model version 2.0 (PDF) is meant to provide federal agencies and other organizations with a roadmap for transitioning to a zero trust architecture and includes five pillars with 'examples of traditional, initial, advanced, and optimal zero trust architectures'.

Per the National Institute of Standards and Technology (NIST), "zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

Zero trust is based on the idea that a breach has already occurred and that no user or asset should be trusted. The goal is to prevent unauthorized access to sensitive assets and to ensure granular access control enforcement.

Implementing a zero trust architecture is a lengthy process that often takes years and incurs additional costs, which faces various challenges, and which requires engagement and cooperation at all enterprise levels.

Achieving a zero trust maturity model involves implementations across five pillars – identity, devices, networks, applications and workloads, and data – and making optimizations over time.



“As agencies transition towards optimal zero trust implementations, associated solutions increasingly rely upon automated processes and systems that more fully integrate across pillars and more dynamically enforce policy decisions. Each pillar can progress at its own pace and may progress more quickly than others until cross-pillar coordination is required,” CISA explains.

Organizations looking to transition to zero trust first need to assess their environments – including systems, processes, infrastructure, personnel, and resources – to identify existing capabilities they can build upon as well as gaps that need prioritization.

According to CISA, for each zero trust pillar, there are four stages to achieving a maturity model, namely traditional, initial, advanced, and optimal, which are combined with three cross-cutting capabilities, namely visibility and analytics, automation and orchestration, and governance.

Achieving maturity for the identity pillar means transitioning to multi-factor authentication (MFA) and phishing-resistant and passwordless MFA, securely integrating identity stores across environments, automating the authorization of just-in-time and just-enough access, and determining identity risk in real time.

Maturing the devices pillar means transitioning from limited or no visibility into device compliance to continuously verifying and enforcing compliance, from not tracking assets to a comprehensive and real-time view of all assets, and from

not having visibility into devices used to access resources to having real-time risk analytics.

Learn more at SecurityWeek's Zero Trust Strategies Summit

For networks, zero trust maturity involves extensive micro-segmentation, dynamic network rules and configurations, encrypting traffic as appropriate and enforcing least privilege principles, implementing proportionate resilience, gaining visibility across all networks, automated configurations and monitoring, and enterprise-wide network policies with dynamic updates.

To ensure zero trust maturity for deployed applications, organizations need to implement continuous authorization of access and real-time risk analytics, advanced threat protections, restricted access to critical applications (over private and protected networks only), robust code deployment mechanisms, application security testing throughout the software development lifecycle, continuous and dynamic application monitoring, and automated app configurations and policies.

Ensuring mature data protections involves continuously inventorying all data, automating data categorization, implementing dynamic methods to optimize data availability, automating dynamic just-in-time and just-enough data access controls, encrypting data in use and enforcing least privilege principles, gaining visibility across and automating the full data lifecycle, and unifying data lifecycle policies.

The new zero trust maturity model document, which integrates the Office of Management and Budget's (OMB) memorandum for a federal zero trust architecture (ZTA) strategy (M-22-09, PDF), is accompanied by CISA's Applying Zero Trust Principles to Enterprise Mobility (PDF) guidance, which describes how zero trust principles can be applied to mobile security technologies.

Related: CISA Gets Proactive With New Pre-Ransomware Alerts

Related: CISA, NSA Issue Guidance for IAM Administrators

Related:CISA Expands Cybersecurity Committee, Updates Baseline Security Goals

CISA Publishes New Guidance for Achieving Zero Trust Maturity