grc outlook

Application Security Viewed Through the Lens of a Zero Trust Architecture

By Sarbari Gupta, Chief Executive Officer, Electrosoft

Office of Management and Budget (OMB) Memorandum M-22-09 "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" offers a detailed approach to implementing a Zero Trust Architecture (ZTA) within the federal government. ZTA envisions both a move away from perimeter defenses and a move toward an operating philosophy where no person, device, network or system is trusted. ZTA seeks to control access and compartmentalize systems or networks so that if an attacker were to gain unauthorized entry the intrusion would be limited to the point of penetration.

Application security thus assumes a fundamental role in the ZTA model. Government agencies must not only view every application as being internet accessible (even if it is not so today) but also implement distinct application security measures. Robust testing is necessary, especially analysis undertaken from the perspective of a potential adversary seeking to discover any vulnerability.

ZTA is not a model reserved exclusively for government agencies, however. Its principles and dictates can and should be applied by private companies and organizations. Viewing application security through the lens of the federal ZTA initiative offers both the framework and rigor needed for any enterprise to enhance its cybersecurity posture.

Inventorying Applications

Detailed knowledge of internet-accessible assets comprising an organization’s system or network is a prerequisite to ZTA implementation. A comprehensive inventory not only defines the attack surface but also facilitates consistent – and thorough – application of security policies. ZTA recognizes that the more complex an organization is, the more difficult it is to identify and track every asset.

Internal records provide a good starting point; however, external scans are often necessary to achieve a complete understanding of an organization’s overall IT infrastructure. Federal agencies can enlist resources available through the General Services Administration (GSA) and the CISA. Private entities can engage the services of website scanning services and similar resources. CISA also can be a resource in many circumstances.

Application Security Features

OMB M-22-09 discusses specific security measures to implement to achieve an effective ZTA model:

- **Multifactor authentication** (MFA) enforced at the application layer. The enterprise must manage all identities accessing its applications. Further, the MFA must ideally use phishing-resistant authentication techniques (such as cryptographic authenticators used with handshaking protocols) to safeguard against inadvertent disclosure of less secure authenticators such as passwords, one-time codes and security questions, among others. OMB M-22-09 describes the World Wide Web Consortium authentication (WebAuthn) and the federal Personal Identity Verification (PIV) standards as effective phishing-resistant approaches. The former utilizes passwordless authentication using public-key cryptography where the key pair resides on the user’s device. The latter employs smart cards using cryptography based on Public Key Infrastructure (PKI). Microsoft's certificate-based authentication in Azure Active Directory also allows phishing-resistant MFA.

- Ideally, authorization-related controls are distinct from measures used to authenticate users. The memorandum speaks to using role-based access control (RBAC) in conjunction with attribute-based access control (ABAC). OMB suggests that the combined approach offers greater assurance than either control individually.
- OMB M-22-09 promotes encryption at several levels. It recommends standard encryption protocols, like TLS 1.3; resolution of DNS requests using encrypted DNS; and encrypting all HTTP traffic. Email encryption is both a goal and a challenge, as no means currently exists to assure encryption across the entire journey from sender to recipient.
- **Logging:** Reviewing and evaluating logged traffic are important features of ZTA. However, ZTA's underlying assumption that any component is subject to compromise yields a warning regarding overuse of monitoring tools as they can constitute a network vulnerability. No such reservation is expressed when it comes to deep traffic inspection of data at rest. Here, traffic volume (users and destinations) is seen to be low and predictable and anomalies readily evident.
- **Application security testing**. ZTA calls on agencies to operate dedicated application security testing programs. Again, the overriding approach is to treat every application as though it were connected to the internet. In addition, independent third-party evaluations should complement in-house testing as outside professionals might disclose issues not raised by staff.

The last element, application security testing, emphasizes the need for rigor, comprehensiveness and application-specific methods. It envisions use of automated and manual approaches as organizations move toward a goal of continuous monitoring and ongoing authorizations. As noted previously, ZTA foresees greater reliance on third-party application security testing to identify vulnerabilities that internal staff may not identify.

The ZTA model also anticipates an expanded role for vulnerability reports prepared by external parties such as security researchers and members of the public. By reviewing and analyzing their findings, agency/organization awareness of potential application vulnerabilities will increase and timely remediation can occur. Relative to cloud platform providers, OMB advises that FedRAMP will interface with providers to assure federal customers can test for vulnerabilities in applications and infrastructure residing on provider platforms.

First Steps

Achieving ZTA, whether in the public or private sector, presents a major challenge. At the same time, it is undeniable that cyber criminals' relentless attacks on government and commercial networks will continue. The potential damage on either front is substantial and unacceptable.

OMB recommends that agencies start with a single application and, using an agile approach, implement the controls that will enable secure operation over the internet within a year's time. Such controls would include provisions for monitoring, safeguarding against denial of service and access control enforcement. Moreover, OMB prescribes that this internet-accessible system be integrated within an enterprise identity management system, which it envisions as a system or systems that automates the management of user identities using metadata drawn from various systems such as human resources, personnel security and contracts management. Beyond reducing staff burden, this approach is seen to benefit uniform policy enforcement and enhance detection of suspicious behavior.

Private entities would be well advised to adopt a similar incremental approach and take full advantage of the federal government's existing standards and guidelines. They prescribe a coherent, logical and disciplined approach to ZTA implementation reflecting expert opinions from government, industry and academia.