Federal Zero Trust Strategy

Eric Mill
Senior Advisor, Federal Chief Information Officer, OMB
eric.r.mill@omb.eop.gov
A mix of short- and long-term work

• Some areas are about taking known, well-standardized technologies, and doing the hard work of implementing them throughout a big organization
  • For example – MFA, encryption
  • Consolidating and federating enterprise identity systems

• Programmatic maturity
  • Vulnerability disclosure and red teaming are not new to agencies, but doing them at the level of consistency and effectiveness we need remains uncommon

• Other areas are about tackling challenging analysis and technology problems that don’t have easily commodified solutions
  • Tagging and classifying data
  • Identifying key security actions and steadily working down the false positives/negatives and building from monitoring (“failing open”) to enforcement (“failing closed”)
A few of our key zero trust priorities

• Encryption in transit
  • Removing implicit trust of the connections between systems
  • Prioritization: HTTP and DNS

• Decryption in transit
  • Bulk decryption with long-lived keys is not compatible with ZT (i.e. use TLS 1.3)
  • Generally, to make context-aware decisions about visibility vs attack surface

• Shifting away from the traditional intranet/VPN model
  • Moving authentication to the application layer
  • Taking the concept of untrusted networks to its logical conclusion
  • Similar to what other security-critical enterprises are doing
  • Need to carve out a safe, supported path to internet-based use of internal systems
A few of our key zero trust priorities

• Phishing and strong authentication
  • Setting a higher bar, while trying to provide more flexibility around PIV
  • Recognizing that apps, RSA tokens, push, etc. do not protect against phishing
  • Making clear that it is okay and expected, today and under current guidance, to have FIDO-compliant devices alongside PIV

• Application security reality check
  • Big emphasis on first/third-party testing and public review
  • Treating everything as internet-accessible
Quick overview of actions – across 5 groups

• Identity
• Devices
• Networks
• Applications and Workload
• Data
Identity

• Phishing and strong authentication
• Consolidation and federation of enterprise identity
• Elimination of old password policies that are known to backfire
  • Periodic password rotation
  • Special characters
Devices

• Endpoint detection and response
  • Not a “rip and replace” approach
  • Coordinating with CISA to establish information sharing
• Reliable asset inventories
  • Taking advantage of dynamic APIs, e.g. cloud services
  • Reliance and participation in CDM
Networks

- Encrypted DNS
  - Either DoH or DoT are supported on phones, browsers
  - Now supported in Windows 11
- HTTPS for “internal” systems
  - Avoiding conflicts between internal and external posture
- Environmental isolation
  - Doesn’t have to be network segmentation, SP 800-207
- Light guidance on decryption
Applications and Workloads

• Heavy application testing
  • Internal
  • 3<sup>rd</sup> party
  • Public vuln disclosure programs
• Bespoke analysis, not generic scanning
• Making an internal application usable over the public internet
Data

- Collaboration between CDOs and CISOs
- Getting started on data categorization and automation of security rules
- Taking advantage of auditability for encryption at rest
- Logging guidance (OMB M-21-31)
Federal Zero Trust Strategy

Eric Mill
Senior Advisor, Federal Chief Information Officer, OMB
eric.r.mill@omb.eop.gov