Executive Order – NIST workshop position paper #3

(Security measures for use of critical software)

Microsoft Corporation

Focus Area

Guidelines outlining security measures that shall be applied to the federal government's use of critical software, including but not limited to, least privilege, network segmentation, and proper configuration. See EO Section 4(i).

Microsoft Response

As part of their operational cybersecurity risk management strategies, organizations should review their environments and determine what's most critical, enabling prioritization of resources reserved for implementing security measures. Many security measures are relevant for both critical and non-critical assets or systems, though the importance of applying those measures may be elevated for critical assets or systems; in addition, to address the unique risk scenarios associated with critical assets or systems, supplemental or enhanced security measures may also be appropriate.

To manage risks associated with the use of critical software, security measures should reflect a holistic approach. Organizations should focus on identifying risks and managing governance processes; protecting data and functions associated with critical software, including through identity and access management, proper configuration management, and software maintenance; detecting anomalies and potential issues; and ensuring readiness of appropriate response and recoverability capabilities. Leveraging posture management tools to continually measure and audit agencies' operational security achievement will help ensure visibility into risk management gaps and focus agency security resources.

Maintaining an inventory of suppliers of critical software and assessing their security posture can help organizations identify risks and manage governance. Numerous existing standards and compliance frameworks and programs can help agencies assess the security posture of suppliers of critical software, including ISO/IEC 27001, FedRAMP, and SOC 2.

Implementation of a vulnerability and posture management program is important to protect data and functions associated with critical software from compromise. For critical software, federal agencies should ensure that software is being maintained (e.g., by suppliers that make lifecycle policy commitments; by agencies in-house as necessary), and they should have programs in place to manage updates, including through testing and verifying the validity of patches or otherwise implementing security mitigations for discovered vulnerabilities.

Along with real-time analytics, use of a Zero Trust architecture, which focuses defenses on users, assets, and resources rather than network-based perimeters,[1] can also support agency efforts to protect, detect, respond, and recover, managing risks associated with deployment of critical software. While criteria for designating critical software is still being defined for federal agencies, central elements of a designation may include enabling access to privileged systems or supporting infrastructure or services for which availability is imperative. In either instance, federal agencies should apply extra resources and

[1] Zero Trust Architecture | NIST

attention toward guarding against, monitoring for, and strengthening recoverability from unauthorized access or disruptions.

A Zero Trust model assumes access attempts may be unauthorized and leverages rich intelligence and analytics to detect and respond to anomalies in real time. To implement Zero Trust principles, organizations must: verify explicitly (always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies); use least privileged access (limit user access with just-in-time and just-enough-access risk-based adaptive policies, implement data protection to help secure both data and productivity); and assume breach (minimize blast radius and segment access, verify end-to-end encryption, and use analytics to get visibility, drive threat detection, and improve defenses).[2]

One way to implement least privileged access for especially critical software is to require the use of a secure workstation to access and use such software. A privileged account management suite of services (e.g., just-in-time entitlement system, password vaulting and rolling solution, and secure hardware platform) to run and access software reduces attack vectors and risks associated with elevated administrative rights, malware, credential theft, and deployment threats. Additional solutions (e.g., VPN, full disk encryption) offer further protection.

Where critical software is being deployed to support the functioning of a critical system or asset, implementation of security measures to ensure recoverability may also be important for ensuring ongoing integrity and availability of those systems or assets. In those instances, federal agencies should ensure that software is able to be updated (i.e., recovered) even when firmware code or critical data are detected to have been corrupted, including through use of guidance consistent with NIST SP 800-193, *Platform Firmware Resiliency Guidelines*.[3]

Recommendations

1. Security measures guidelines should incorporate key practices across the identify, protect, detect, respond, and recover functions as described in the NIST Cybersecurity Framework,[4] including governance of suppliers of critical software; vulnerability management programs; proper configuration; and technologies and processes to enhance recoverability of critical systems and assets.

2. Security measures guidelines should reference the importance of implementation of each aspect of a Zero Trust model:
   - Verify explicitly – Modern identity and access management technologies and processes should be required for agencies to use critical software, including technologies and processes that explicitly verify both users and devices.
   - Use least privileged access - Among federal employees and any others with access to critical software, such access should be limited by just-in-time and just-enough-access principles.
   - Assume breach – Agencies should use intelligence and analytics to improve threat detection and deploy segmentation and isolation of resources to minimize the “blast radius” in the event of an incident.

[2] Zero Trust Security Model and Framework | Microsoft Security
[3] SP 800-193, Platform Firmware Resiliency Guidelines | CSRC (nist.gov)
[4] Cybersecurity Framework | NIST