IAD's Top 10 Information Assurance Mitigation Strategies

December 2015

Fundamental aspects of network security involve protection, detection and response measures that can be grouped into four mitigation goal areas. These four mitigation goal areas target critical steps in the intrusion life cycle — creating a technical layered defense approach that supports the ability to "fight through" a contested cyber environment:

- **Device Integrity**—maintaining and measuring device health/integrity. Devices often represent the attack surface area or the persistent living-space for the advanced persistent threat (APT).
- **Damage Containment**—when intrusions occur, limiting losses of information, systems, and mission capabilities.
- **Defense of Accounts**—protecting credentials from misuse and enabling trusted authentication and access.
- **Secure and Available Transport**—maintaining the privacy and reliability of data communications.

These goal areas will support current and future cyber defense efforts, helping to set priorities, and contributing to the desired end-state of denying adversaries the ability to operate on our networks and impact our missions. Efforts that can be implemented now are listed below as IAD's Top Mitigations with goal areas indicated in the left margin. By blocking critical points in the attack life cycle, these mitigations are effective against entire classes of attacks, including new unknown variants.

1. Application Whitelisting:

Application Whitelisting is a proactive security technique that allows a limited set of approved programs to run, while all other programs and most malware are blocked from running by default. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

2. Control Administrative Privileges:

Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are restricted from normal users. Network owners should only grant Administrator privileges when absolutely necessary and should take steps to ensure Administrator accounts are not exposed to the internet and other sources of increased risk. More robust protections can be achieved through the use of two-factor authentications for administrators and other privileged accounts.

3. Limit Workstation-to-Workstation Communication:

Pass-the-Hash (PtH) is a hacking technique that allows an attacker to authenticate to a remote system by using the underlying hash of a user's password rather than having to know the actual password itself. Hackers generally use hashes from the current machine to springboard to other machines, grabbing higher privileged credentials as they progress. A range of security measures are required to fully mitigate all the facets of Pass-the-Hash. One scalable and highly effective mitigation involves limiting workstation-to-workstation communication, thereby thwarting an attacker's ability to leverage PtH to move laterally within the network.

4. Use Anti-Virus File Reputation Services:

Most of today's host security products augment their product's core host controls with intelligence from cloud-hosted threat databases. In order to gain the most complete threat picture, organizations need to leverage these threat intelligence clouds.

5. Enable Anti-Exploitation Features:

Many operating systems and applications have advanced antiexploitation and sandboxing features that should be harnessed to defend against common attacks. For example, in Windows, the Enhanced Mitigation Experience Toolkit (EMET) is a host-based application that hooks into processes and watches for common memory exploitation techniques, such as buffer overflow attacks. When EMET detects an exploit attempt, it promptly kills the targeted process, logs the attempt, and notifies the user that it has shut down the application. EMET offers fundamental protection against common classes of exploitation used as building blocks of zero day attacks.

6. Implement Host Intrusion Prevention System (HIPS) Rules:

Standard signature based host defenses are overwhelmed by exploit kits that continually morph attack components. HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities. For an enterprise with a well configured and managed network, HIPS can be tuned to learn and allow normal network functionality while flagging anomalies characteristic of intrusions.

7. Set a Secure Baseline Configuration:

Perhaps the most scalable way to control an enterprise's attack surface is through secure host baselines. This includes generation of standard images which provide approved and secured application and operating system configurations with layered security containing best practice mitigation strategies to counter cyber threats.

8. Use Web Domain Name System (DNS) Reputation Services:

Various commercial services offer feeds rating the trustworthiness of web domains. Enterprises can protect their hosts by screening web accesses against such services and redirecting dangerous web requests to a warning page. Inspection can be implemented at either the web proxy or browser level.

9. Take Advantage of Software Improvements:

Operating systems and application software routinely have security upgrades through new versions and intermediate patches. Apply these updates in a timely manner to reduce vulnerability exposure and maximize software reliability and protections.

10. Segregate Networks and Functions:

Plan for the possibility of a successful intrusion and design the network architecture and management procedures to separate segments based on role and functionality. Closely monitor the interactions between the sections, so that a compromise of one part can be detected and does not directly lead to the compromise of others.

Contact Information

Industry Inquiries
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov