Software Asset Management:

A Key Element of Computer Network Security and Attack Mitigation

Abstract:
Network security is an often-overlooked aspect of Software Asset Management, but a comprehensive SAM program can provide the foundation for preventing and reducing the adverse impacts of cyber-attacks on critical systems. Federal agencies are developing new standards-based processes that rely heavily on SAM to meet the following challenges: Identifying software that is installed on all devices - including legacy and end-of-life products; verifying that media is authentic and has not been tampered with; determining any software that was installed via unauthorized methods and restricting the execution of this software; and identifying flaws in deployed software and any patches that must be installed to remedy them. Establishing a complete, accurate software baseline provides a means of meeting these challenges. SAM managers need to be aware of these activities and understand their potential responsibilities around network security.

Background

Software Asset Management (SAM) involves more than the typical focus of ensuring compliance with license agreements and avoiding costly software audits. A comprehensive SAM program can have a significant positive impact on an organization's network security as well.

An organization's structure, governance and essential business functions and processes are highly dependent upon information technology. That technology is directed through the use of software of many types. It is critical that organizations deploy software based on sound architectural approaches that support both operational and security needs to protect the confidentiality, integrity and availability of information and systems.

Historically, network security has not been a primary concern of Software Asset Managers. However, that is likely to change in the near term, as attacks on networks are becoming more common and increasingly sophisticated. It is essential that Software Asset Managers in both the government and private sectors are aware of evolving security initiatives, and that they bring that awareness to their organizations. Many of these initiatives are based upon activities that SAM managers practice daily: software procurement, software discovery, software updates, asset identification, and vendor communications.

Primary Software-Based Threats to Network Security

Defects and Vulnerabilities

A major issue confronting organizations is ensuring that all purchased and deployed software is secure, and that it is free from malicious functionality and defects that may invite intrusion. Software is purchased from publishers who assure that their software will provide the intended functionality and not harm the enterprise. If any vulnerabilities or defects are discovered, it is expected that these will be identified and that patches or updates will be published. Identifying and responding to new vulnerabilities, evolving threats, and an organization's constantly changing security and operational environment is a dynamic process that must be effectively and proactively managed.

Stealth Modification of Functionality

Another emerging threat is unauthorized modification of existing deployed software to enable unintended functionality. Previously approved and verified software that is deployed in an organization can be stealthily modified to perform functions that can facilitate the theft of data and assets or affect the organization's ability to continue operations. These modifications can enable remote control, steal data, and disrupt operations in a manner that is difficult to detect.

It is important to note that common virus scanning processes are unlikely to detect modifications to deployed software, due to the nature of the changes. Systems that can detect stealthily modified software are essential to network security. This detection functionality is provided in certain software discovery processes that are currently used in SAM programs. Therefore, organizations that are using these select tools may already have the functionality and expertise to identify these threats.

Unauthorized Installation Methods and Sources

An additional verification step to ensure network security is to identify the method of software installation as well as the original source. It is possible to track installation paths to ensure that all software was installed via approved methods, whether it was completed via a software distribution package or an authorized manual installation. This verification may be completed via reporting from the software distribution tool itself, or from later discovery scans that determine installation paths and destinations.

Additionally, digitally signed software ID (SWID) tags will increasingly be used to identify authorized installations. Conversely, the absence of digitally signed tags will help to reveal unauthorized installations. It is also possible to compare the attributes of installed software to the attributes of the authorized installation package to ensure that the installed product is authentic and unaltered from what was provided from a publisher in the original source.

Prevention and Mitigation Initiatives

These software-centric network security issues are drawing the attention of organizations that are at high risk, as well as those who wish to reduce their level of vulnerability. As a prime example, the U.S. Department of Homeland Security (DHS) has stated that cyber-attacks on Federal government networks are growing more sophisticated, aggressive, and dynamic. Government computer networks and systems contain national security and law enforcement information, and other sensitive data including details about federal employees and others. It is paramount that the government safeguards this information from theft and protects networks and systems from cyber-attacks while continually providing essential services to the public.

To do so, the DHS is launching an initiative known as the Continuous Diagnostics and Mitigation (CDM) program. This program outlines a dynamic approach to fortifying the cyber-security of computer networks and systems. As the department responsible for securing unclassified federal civilian government networks (the “dot-gov” domain), DHS coordinates the national response to significant cyber incidents and maintains a common operational picture for cyberspace across the government.

The CDM program that is being adopted by the U.S. Government is a precursor to programs that will almost certainly be adopted by non-government organizations. All non-government organizations are likely to be impacted, especially those in banking, finance, utilities, pharmaceutical and heavy industries. It is essential for SAM managers to understand and provide leadership in this particular aspect of software assurance.

Pillars of the CDM Process

Specifically, the CDM program encourages risk-based decision-making and automated action. This requires accurate, timely information about the current state of the software that is authorized, installed and used on computing devices (also called endpoints), accessing organizational resources and supporting critical business functions.

Multiple levels of software discovery should be used to detect and profile each system on the network, as well as associated traffic, to determine which systems are active or idle. This provides full and constant visibility into network usage. Any new installations or configuration changes are detected and made visible, allowing the state of the device to be re-assessed quickly.

The automated collection and secure exchange of software inventory data enables process automation in several areas that support this initiative. The first area is around authorization for the installation and execution of software,. The second is the understanding of which patches and software updates are needed to minimize vulnerabilities, and finally, the determination of which software configurations need to be applied to ensure compliance with organizational configuration policies.

The CDM program and others like it should include pre-determined, quantified "risk scores" that determine threat levels. Appropriate responses, whether automated or involving human intervention, should be clearly outlined in advance. Continuous feedback improves the effectiveness of the program by enabling policies to be adjusted as required.

Solutions for Detection, Remediation and Enforcement

Tools that are currently used to support SAM programs can help maintain a baseline inventory of software that is installed and used within the organization. This can be accomplished with a combination of system configuration, network management and license management tools, or with other special-purpose tools. These tools can help track the lifecycle of an organization's software assets, and they provide capabilities such as remote management of devices and other automated management functions. The implementation and effective use of SAM solutions is a key component required to assist organizations in automating the implementation, assessment and continuous monitoring of software-related security controls such as those found in NIST Special Publication (SP) 800-53 Revision 4 and ISO/IEC 27001:2013.

In order to address and overcome issues that may arise with the use of discovery tools alone, NIST is suggesting the use of Software Identification (SWID) tags to simplify the complex task of maintaining an accurate software inventory. Discovery tools can provide challenges around platform support and software identification accuracy and consistency. When these issues are compounded by the use of multiple discovery tools within a network environment, achieving the proper level of data reconciliation may be difficult.

By design, Software Identification (SWID) tags record unique information about an installed software application, including its name, edition, version, whether it's part of a bundle and more. Additionally, a secure digitally signed tag process makes it possible for an organization to supplement any publisher-provided tags with information that will provide a more complete picture of the software environment. The presence of a particular tag can clearly mark that an installation was derived from a proper source and was installed via an approved channel. Tools that allow the creation of digitally signed software tags ensure that each tag's creator is clearly identifiable. This reduces the possibility of fraudulent tags being created, which may be linked to unauthorized or modified software.

How Eracent Meets The CDM Challenge

Eracent's solutions have a proven ability to fulfill all of the aspects described above in very large, complex and secure environments. Eracent's Software Base-Lining, Application Mapping, and Software Identification (SWID) Management processes meet the intent and satisfy the design requirements of CDM.

Software Base-Lining

Eracent's ITMC Discovery toolset provides comprehensive detection of hardware and installed software across multiple platforms, and helps to establish a digitally signed baseline from which to make ongoing comparisons. Eracent's Software Base-Lining process is currently being used by major secure enterprises worldwide to mitigate the possibility of stealth software modifications.

Installation paths are detected, verifying that authorized sources and approved installation methods were utilized. If abnormalities and exceptions are detected, the Eracent system can be used to automatically remediate the problem by deploying patches or removing affected software, either directly or in conjunction with other distribution technologies that are in use.

Application Mapping

Knowing where specific software is deployed to support specific process applications (e.g.,. Oracle databases for a financial system) is essential for maintaining process security and availability. Eracent's Application Mapping and Configuration Management processes provide the means for users to maintain CIs, enabling them to properly assess the potential impact of cyber-attacks and prioritize remediation tasks. The data collected through the application mapping process will also identify unauthorized communications to potentially rouge systems and applications.

Software Identification (SWID) Tag Management

Secure, digitally signed SWID tags may be created for packages and distributed to all associated installations. SWID tag information may be read from each installation and reported in conjunction with all associated system data. Management of SWID tags is accomplished through Eracent's capabilities around reading and also generating secure digitally signed SWID tags. Eracent has been closely involved with the SWID process as a member of the ISO/IEC 27001-2 committee since its inception. The security around tag generation and assurance is a major part of the CDM process.

All of these functions can help Software Asset Managers meet the increasingly important requirements that are necessary for a secure network infrastructure. For a more detailed look at Eracent's comprehensive IT Asset Management and Software Asset Management solutions, contact Eracent today

Bibliography:

Websites:

http://www.dhs.gov/cdm

http://www.gsa.gov/portal/mediaId/180247/fileName/CMaaS_Ordering_Guide_V30_Oct2013

http://csrc.nist.gov/nccoe/Building-Blocks/conmon.html

http://csrc.nist.gov/nccoe/Building-Blocks/Continuous%20Monitoring%20Building%20Block%20-%20Software%20Asset%20Management.pdf

http://tagvault.org/swid-tags/

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53670

http://www.mcafee.com/us/industry/public-sector/continuous-monitoring.aspx
http://www.mcafee.com/us/resources/solution-briefs/sb-embrace-continuous-monitoring.pdf

http://en.wikipedia.org/wiki/Software_assurance

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

http://scap.nist.gov/events/2012/itsac/presentations/day1/3Oct_430pm_Klos.pdf

http://scap.nist.gov/events/2012/itsac/presentations/

http://en.wikipedia.org/wiki/ISO/IEC_27001:2013

http://en.wikipedia.org/wiki/ISO/IEC_19770

Articles:

- DHS contract looks to bolster civilian cyber defense — Federal Computer Week (8/13/2013)
- With $6 billion continuous monitoring contract, DHS takes ‘next leap’ in cybersecurity — FedScoop (8/14/2013)
- 17 companies will participate in $6 billion ‘continuous diagnostics’ contract from DHS — Government Security News (8/13/2013)
- DHS 'continuous diagnostics and mitigation' program offers cybersecurity model for companies — Inside Cybersecurity (10/25/13)
- DHS Awards Contractors $6 Billion for Agency Network Surveillance — NextGov (8/13/2013)
- 17 win $6B DHS continuous monitoring contract — Washington Technology (8/13/2013)
- DHS Awards $6 Billion Cybersecurity Contract To 17 Vendors — Homeland Security Today (8/14/2013)
- DHS to standardize cyber protections through new contract — Federal News Radio (8/13/2013)

www.eracent.com

USA Headquarters:
8133 Easton Road
Ottsville, PA 18942
United States
Phone: +1- 908-537-6520