GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Reguly, Tyler

Title: "20 CIS Controls: Control 3 – Continuous Vulnerability Management"

Website: Tripwire Blog

Organization: Tripwire

Date: 30 April 2018

URL: https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-3-vulnerability-management/

Accessed: 15 July 2019

Synopsis: Today, I will be going over Control 3 from version 7 of the top 20 CIS Controls – Continuous Vulnerability Management. I will go through the seven requirements and offer my thoughts on what I've found.

Key Takeaways for Control 3

- Takeaway 1. A robust, vulnerability management program powered by the correct tools will empower your organization to take control of its own security and manage risks presented by both internal and external threats.
- Takeaway 2. Utilizing remote and credentialed scans gives you a holistic view of your network that allows you to better understand threats before they become a problem. When you review and compare your results, you will quickly know what has changed and what risks those changes introduce.
- Takeaway 3. Vulnerability management programs, when properly implemented, expose a plethora of faults and flaws in even the most secure enterprises networks. Don't be alarmed; simply apply risk-ratings and break the work into smaller, more manageable portions.

20 CIS Controls: Control 3 - Continuous Vulnerability Management

Today, I will be going over Control 3 from version 7 of the top 20 CIS Controls – Continuous Vulnerability Management. I will go through the seven requirements and offer my thoughts on what I've found.

Key Takeaways for Control 3

- **Takeaway 1.** A robust, vulnerability management program powered by the correct tools will empower your organization to take control of its own security and manage risks presented by both internal and external threats.
- **Takeaway 2.** Utilizing remote and credentialed scans gives you a holistic view of your network that allows you to better understand threats before they become a problem. When you review and compare your results, you will quickly know what has changed and what risks those changes introduce.
- **Takeaway 3.** Vulnerability management programs, when properly implemented, expose a plethora of faults and flaws in even the most secure enterprises networks. Don't be alarmed; simply apply risk-ratings and break the work into smaller, more manageable portions.

Requirement Listing for Control 3

1. Run Automated Vulnerability Scanning Tools

Description: Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

Notes: Regular automated scanning is important to keep informed of new vulnerabilities and changes being introduced across networks. Weekly scans are adequate for less critical systems, but the more frequent the scans, the sooner issues can be noticed and resolved. Automated scans give valuable insight into the current status of all scanned systems to help prioritize which vulnerabilities are most compromising the security of the network.

2. Perform Authenticated Vulnerability Scanning

Description: Perform authenticated vulnerability scanning with agents running local on each system or with remote scanners that are configured with elevated rights on the system being tested.

Notes: Performing authenticated vulnerability scans produces much more accurate audit results because it comes down to data and information. Unauthenticated scans can only gather data related to what the scanning tool can "see" from the outside of

the endpoint. On the contrary, authenticated scans allow the tool to gather information from both the outside and the inside. Data from both of these perspectives is important, but the data gathered from the inside via authenticated scans allows the scan tool to make far better analysis of the endpoint's vulnerability state.

3. Protect Dedicated Assessment Accounts

Description: Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.

Notes: Vulnerability scans should always use dedicated credentials with the absolute minimum level of privileges required for scanning. This will minimize the risk of credential theft while also facilitating more effective SIEM practices. The goal is to make any use of scanning credentials for something other than scanning stand out to analysts.

4. Deploy Automated Operating System Patch Management Tools

Description: Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

Notes: This requirement, in many cases, is good practice. The use of such automated tools often allows users to patch critical security holes as soon as fixes are made publicly available. However, it is important to be mindful of the fact that operating system updates often require a reboot in order for the vulnerability in question to be fully patched. Performing an automatic reboot would likely be deemed undesirable in high availability environments. System administrators must be particularly diligent in these environments by scheduling appropriate maintenance windows to ensure that patches are applied completely.

5. Deploy Automated Software Patch Management Tools

Description: Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the vendor.

Notes: Automated software update tools are great because they can be more consistent and less error-prone than manual updating. However, this is not a fire-and-forget type of situation: not all third-party software will play nicely with every automated software update tool, and there are still firmware updates to worry about. Making assumptions about automatic updates can leave you with gaps in your perimeter. They're a great solution, but there will still be (manual) work to be done.

6. Compare Back-to-back Vulnerability Scans

Description: Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

Notes: Regular vulnerability scans ensure that all known high risk vulnerabilities are

found within an organization, which allows them to prioritize mitigation of high risk vulnerabilities found on their systems. Furthermore, it enables the administrators to determine if systems have critical patches installed. This process allows organizations to minimize their exposure to potential attacks for known critical vulnerabilities that are on their systems.

7. Utilize a Risk-rating Process

Description: Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

Notes: Trying to fix everything at once creates a non-starter. Everyone knows that you cannot jump into a massive project without breaking it down. The best way to breakdown your vulnerability reports into manageable tasks is to utilize a risk-rating process and start with the highest rated tasks. This allows you to make forward progress on the highest risk vulnerabilities without feeling overwhelmed. It also gives you a measurement tool for how well you're progressing and how quickly your remediation efforts are applied.

See how simple and effective security controls can create a framework that helps you protect your organization and data from known cyber attack vectors by downloading this guide here.

Read more about the 20 CIS Controls here:

Control 20 – Penetration Tests and Red Team Exercises

Control 19 – Incident Response and Management

Control 18 – Application Software Security

Control 17 – Implement a Security Awareness and Training Program

Control 16 – Account Monitoring and Control

Control 15 – Wireless Access Control

Control 14 – Controlled Access Based on the Need to Know

Control 13 – Data Protection

Control 12 – Boundary Defense

Control 11 – Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Control 10 – Data Recovery Capabilities

Control 9 – Limitation and Control of Network Ports, Protocols, and Services

Control 8 – Malware Defenses

Control 7 – Email and Web Browser Protections

Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs

Control 5 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Control 4 – Controlled Use of Administrative Privileges

Control 3 – Continuous Vulnerability Management

Control 2 – Inventory and Control of Software Assets

Control 1 – Inventory and Control of Hardware Assets

You can also learn more about the CIS controls here.