James Everett Tourtellotte IV
ITN 262
W. McLaughlin
9/18/2022

One way compliance laws and business drivers for Health Care Provider's Workstation Domain differs from DoD's Workstation Domain Security Compliance revolves around the concept of proactivity vs. reactivity. When you navigate to https://www.hhs.gov/hipaa/ and click on the hipaa for professionals section, you will see a tab that will tell a professional what to do if a cyber attack occurs. This document entails a list of steps, arbitrary for the point at hand, that are all reactive countermeasures to a cyberattack. Not a single one revolves around a proactive measure to prevent a cyber attack. This significantly differs from the DoD's Workstation Domain compliance requirements, which is proactive. The DoD's requirements revolve around STIG, or Security Technical Implementation Guide. STIG is a configuration standard that the DOD uses to lock down information systems that might otherwise be vulnerable to a cyber attack. This standard likely has a plethora of specific countermeasures that are arbitrary to the point at hand. Simply put, the STIG, is proactive against cyber attacks - or at least attempts to be.

In terms of risks, threats, and vulnerabilities CIO.com outlines 10 commonly found in workstation domains. First risk is USB Devices. This risk can date back to 2005, where a Yankee Group Survey found that 37 percent of companies reported that USB devices were believed to be the cause of compromised corporate information. Next, we have peer-to-peer file sharing programs. These are programs that have made their way into corporate in mass, but continuously cause risk to companies. Check the P2P DDOS Attack called dc+++, that compromised roughly 300,000 computers. Next we have Antivirus problems, which we will bundle this risk with Outdated Microsoft Service Packs and Missing Security Agents. Both of these risks revolved around the basic security principle of automatic updates. These problems

all arise when workstation domains are not properly updated or outfitted with the latest updates. For example, Code Red Worm infected 359,000 computers in 14 hours via a vulnerability in windows that had been patched two years prior to its existence. Next, we have unauthorized remote control software. This is a risk that revolves around integrity. Remote Control Software is sometimes very crucial to a business' operation, however if the installation is rogue - it can provide a threat to your workstation. Another risk CIO outlines is Media Files. These are variables that increase your attack surface. Whether it is a workstation, or a website, malicious actors can hide spyware, trojans, viruses, and more within media files through steganography or other techniques. Next we have Unnecessary Modems. CIO entails that a wide variety of modems, commonly prebuilt into older systems, are not covered by a company's firewall. This opens up an attack surface if the modem is connected to the internet, while not protected. The last two threats and/or risks revolve around Wireless connectivity. Unauthorized synchronization software can provide an opening for attackers to penetrate a workstation domain, then god forbid your network. Then, with wireless connectivity you have the risk of lacking endpoint security.

I was able to learn about a few of the overarching DoD Standards for desktop hardening. The first standard, revolving around Public Instant Messaging Clients being installed, was very classic. Its direction was simple - Public Instant Messaging Clients will not be installed on Desktops. The document entails that it is simply another attack surface, but specifically one that could end up carrying confidential messages. Because of that threat, the decision is to simply not allow these types of clients on a Desktop. The second concept that stuck out to me was the Execution of Restricted File Type Properties. It immediately outlined that you never want to have a Desktop that is vulnerable to remote code execution. Files of all kinds can be an attack vector. Their remediation was fascinating however, forgive me for the following ignorance

- it appears one way to prevent this without banning filetypes is hardening the workstation domain through automatic processes. They entail a windows command that would prompt a warning for a user, in hopes it would allow the user to see the full file name to ensure it is the correct extension - before they even view or execute a file. It also states that all file extensions should be viewable. This would again, harden the desktop by allowing the user to know exactly what file they are clicking on - the principle of integrity.

Removable media devices, per the Windows 10 STIG, show to be a potential attack vector if the workstation is not hardened via disabling autoplay. This feature leaves a system open to attack via USB if it can be simply plugged in and the computer runs it itself. Whether you disable this through a command or with a tool, security configuration is a must. The Windows 10 STIG outlines a wide variety of Security Tool Configurations across a wide variety of applications. TELNET, TFTP, Auditing Configurations, and more are all mentioned here. What appears to be a security configuration would be the halt of a system if it fails an audit. The display of a shutdown button also appears to be one of these security configurations. This could be used in the case of a need to remotely shutdown a workstation - by an administrator in this case.

Risk can be mitigated through an AUP a few ways by using the STIG for the related system. In the case of this exercise the Microsoft Windows Server 2016 STIG was the focus. One means of use policy for hardening involves changing your password every 60 days, and requiring compliance of password complexity be met. They also have guidelines such as limiting the permissions non-admins or groups have on printer shares. This AUP revolves around the least privilege principle. Another AUP revolves around dormant or not used accounts. A few of

these hardening techniques differ, one involves disabling unused accounts that are over 72 hours old.

The US NVD Database houses its vulnerabilities through a search query. One can search for a product name, vendor name, CVE name, or an OVAL query. The reason this is a security tool and also an attack tool is it can help both sides. A blue team would use this for threat research and eventually begin remediation steps for a system that is affected. A Red Team would use this to query a CVE of a potentially vulnerable system, to get a lead on how to execute the payload. It could start with a search on this database, and end with one downloading a python script from exploit.db.