Jackson Warren

Jeremy Bergen

CSCI 370

9/10

Week 2 Lab

Looking into the differences in workstation security between the health care client and the DoD client, we see that both have somewhat strict regulations on their release of information. HIPAA is more centered around singular persons, and release of their information has to be very secure and confidential, while the DoD client would need protection for entire systems. I also imagine the DoD client would need much more secure logon credentials based on different access levels, while the HIPAA client might be more access or no access. However, DoD does not require a third-party audit, while HIPAA does. Business drivers for both companies would be somewhat similar being a company trying to secure information. The health care company would be security of personal information and documents, and the DoD would likely be general company information and activity. Both would have very similar risks with information leaks, backing up information, and logons/passwords security.

References:

Complyup. (2021, July 20). *Compliance Overview | CMMC & NIST 800–171 | ComplyUp*. Compliance Assessment Platform | ComplyUp. https://complyup.com/compliance-overview/?utm\_campaign=CU20+-+Static+CMMC+Search+Campaign&utm\_source=adwords&utm\_medium=ppc&utm\_term=dfars%20compliance%20requirements&hsa\_acc=8381633541&hsa\_cam=11146093633&hsa\_ver=3&hsa\_net=adwords&hsa\_src=g&hsa\_tgt=kwd-818563094323&hsa\_grp=106544827862&hsa\_ad=465972905277&hsa\_kw=dfars%20compliance%20requirements&hsa\_mt=b&gclid=CjwKCAjwj8eJBhA5EiwAg3z0m\_21XmPe\_Aw0SjAU9D4z3QOyW-y7E-yVNAl8Ao5sWF2ZU1yOIhfRNhoC-V8QAvD\_BwE

Weaknesses and threats to workstation systems include hardware manually connected to the system that compromises the system, file sharing (P2P) creating informational leakage problems, lack of sufficient antivirus software leading to unexpected failure in protection, running systems on older versions of Microsoft leaving gaps in updated securities, lack of security agents leading to a lack of network monitoring, unauthorized access to remote-control privileges of a computer, giving them full access and control of a user’s device, personal photo and video due to the fact that it can easily contain malicious cargo through metadata, unneeded modems, synchronization software that leads holes and unknown downloads in the background, and finally, lack of protection to wireless connections.

For answers relating the xml files, I was unable to open said files. I used <https://www.stigviewer.com/> to gather info and discuss the topics. I focused less on the identification and classification of the topics and more on important points and discussion for those topics mentioned:

* Public instant message clients are installed – Rated a CAT 2, public instant messaging is a threat due to the fact that it is routed in a public domain. Consequently, these messages can end up being intercepted while traveling through this domain, revealing private/sensitive information. Possibly less problematic than some other security threats, an easy solution is to find a more secure way of communication that does not utilize the public domain or has more protections when traveling through the public domain.
* Peer to Peer clients or utilities are installed – Rated at a CAT 2, P2P is mostly severe due to the misuse/potential of file-sharing abilities among employees/users. Loss of sensitive data is a threat, as well as legal implications of infracting on sharing files also creates many issues very quickly.

------------------------------------------------------------------------------------------------------------

* Display Shutdown Button – CAT 3, ensuring the security of authorized system shut down and anonymous shutdown. This is a low threat, and somewhat easy to ensure based off the user of the system. Hiding the misuse of this is also somewhat difficult, as it will be logged in the system security automatically.
* Clear System Pagefile – CAT 3, this ensures that Windows will not wipe the system pagefile on a controlled shutdown. While this is important for not losing memory, it is not a large threat and does not usually have large repercussions.
* Removable media devices – This one has ranging risks associated with it, from CAT 1 to CAT 3. The incorrect use of an external media device could pose huge threats to a system, leaving it susceptible to attack and loss of private information. On the other hand, training and understanding procedures to avoid this is somewhat simple, and if done correctly, this can lower the risk.
* Halt on Audit Failure – With a CAT 2, Halt and Audit Failure is also a very important aspect of a working system. If there are errors, the system has several safe guards, such as overwriting older audit records and queuing audit records locally till communications with the audit server is restored.
* Security Configuration Tools – CAT 3. This is a somewhat low threat since it is a single configuration file for security systems. This then is able to be applied for other machines. This is higher level access only, and not as easy to alter due to this.

------------------------------------------------------------------------------------------------------------

* System Recovery Backups – Users can use hardcopy backups, reducing security risk substantially when backing up information. However, this is not very practical, so requiring users to implement a secure and trusted backup server for system recovery is recommended and would follow AUP.
* Caching of Logon Credentials – Companies should ensure that caches for logon’s are limited, as well as protected. Lowering the number of stored logons in a cache to reduce risk is a solution, or even eliminating the idea as a whole, even though that would have several downsides as well. To follow AUP, admins would have to make expectations with these caches clear.
* Dormant Accounts – Companies should disable accounts that have not been active for around 30 days. Then, if still inactive after 45 to 60 days, accounts should be deleted. This leaves less loose ends where people could take advantage of dormant accounts. Having this timeline defined will also respect AUP guidelines.
* Recycle Bin Configuration – This should follow similar guidelines to the last. Deleting information has to have safeguards incase information is accidently deleted, but it must be fully deleted within a timeline so it is not recoverable later putting it at risk. Again, a similar 30-day rule might be applicable here to reduce risk while not negating the benefits of the recycle bin.
* Password Uniqueness – Requiring unique passwords is very important and easy to follow with AUP. Stating that users must follow specific guidelines when creating passwords is easy to do, and reduces risk significantly.
* Printer Share Permissions – Admins would most likely want to ensure they had good security systems installed for printing services for all employees. Employees must agree to use that software and that software alone for printing purposes. This could create conflicts with different printers, but there is solutions to this that would not risk security.

CVE is a website that seeks information and solutions on vulnerabilities to many tech problems. They collect known vulnerabilities, and publish them free for people to use. By going on to CVE, you can request an CVE ID using a web form where CVE employees can identify the vulnerabilities you might be facing with your system, and find potential solutions using their databases. Specifically, for Workstation Domain OS and Software Vulnerabilities, CVE will have specific ID’s related to these vulnerabilities, references on the issue, and a description of the vulnerability housed in their databases. By searching for a keyword, users can find similar/exact vulnerabilities they are having with their system, and look for potential solutions from the references or CVE. CVE also can help narrow in on your vulnerabilities by using the request form mentioned earlier. These files are then offered/housed in a number of formats (HMTL, CSV, txt, or xml), either zipped, compressed, or raw.

Vulnerabilities are stored as a CVE file, just as before, with identification numbers, references, and description of said vulnerability. Then, these CVE files are added to an NVD database that builds upon the CVE database. This database includes more exact data, such as fix information, severity scores, and impact ratings. It even adds several searching features making it easier to find. While this is a great resource and will help make problems more known and easier to solve with more information in the cybersecurity realm, it also helps hackers. Hackers will be able to know exactly how to exploit these vulnerabilities for companies that haven’t fixed these issues. So even though it is helpful to those utilizing CVE and implementing the changes needed to patch these vulnerabilities, it leaves a lot of room for damage by people exploiting these documented issues.

The major workstation domain risks and threats I found in this study are removable media devices, caching logon credentials, and lack of sufficient antivirus equipment. Removable media devices are always a huge threat. They can break the security of the company’s workstation domain, store private information, and more. Mitigation would be very clear and strict ruling, requiring employees to not abuse said media devices and understand exactly what is appropriate for these media devices. Logon credentials is another large security vulnerability that needs to be considered by companies to protect their users’ information and passwords. Ensuring that their caches are limited will reduce this threat, while the company must make sure users are aware of the mitigations put forth. One of the main ones a workstation domain will be lacking is antivirus equipment. This can reduce risks and vulnerabilities greatly – if utilized. So, in order to ensure this is the case, the company will have to automatically mandate updates to the chosen antivirus software, confirm all employees have it installed and updated, and make employees aware they must be using this software to mitigate this risk.