**Second Attempt -- Discuss what security measures you have implemented or will implement as a result of this unit**

This unit has raised my awareness of the need to secure computer networks; and considering I only have access to my own home network, I will discuss the best-practice security measures that the NSA recommends in their guide for home networks as well as security measures already in place on my home network. The NSA recommends using an up-to-date operating system and performing automatic updates or patching it often in order to ensure the latest security measures are in place. I am currently running Windows 8 and have no intention of upgrading any time soon. Our router is set to pass through, but we have a separate firewall installed inside of that and use WPA2 encryption for authentication on our home network. In addition, we have separate internal networks for traffic on our router; we use our 2.4G network for riskier machines (guest users, phones, my laptop which doesn’t even run antivirus) and this network cannot be used reach the router or other network. Our hidden 5G network hold only 1 machine with all of our financials, and this is the only machine that has administrative privileges for the firewall and router. For the most part, we try to use behavioral best practices to reduce our vulnerability to attacks: like not opening links and attachment from questionable email sources, not downloading from disreputable websites, using tough to hack passwords and changing them periodically, and not using public hotspots to log into anything sensitive. As for storage, nearly all of our storage is done on google drive and dropbox; and so, when any devices on our network behave weird: slow, frequent crashing, etc (which is rare), we simply restage the machines to factory to make sure our devices are clean and then change passwords. If we had unlimited funding, we would upgrade our devices and operating systems frequently as well as subscribe to antivirus software, but we have other priorities with family in mind.

References

NSA/CSS (2018). Info Sheet: Best Practices for Keeping Your Home Network Secure. *United States of America National Security Agency.* Retrieved from

<https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf?v=1>

**First Attempt -- Discuss what security measures you have implemented or will implement as a result of this unit**

The Operating System virtualizes memory, not only to make processes run efficiently, but also to keep potentially dangerous processes from disrupting other processes or even taking over the system (Arpaci-Dusseau & Arpaci-Dusseau, 2012). Considering the extent to which devices are networked, “it is no surprise that developers have implemented a variety of defensive countermeasures to halt those wily hackers from gaining control of systems” (Arpaci-Dusseau & Arpaci-Dusseau, 2012). One method to thwart hacking, is to monitor systems and networks for malicious activity and benign events that could leave systems vulnerable to attack (NSA/CSS ,2013). In other words, logging system activity for proactively monitoring the custom views of the logs on a daily basis or plugging the logs into a Security Information Event Management (SIEM) system can help an administrator determine if a system is at risk or if it has already been compromised so that action can be taken to rectify the situation. According to the NSA/CSS (2013), the first step in logging system activity should be to deploy a clean, and therefore uncorrupted, dedicated server whose sole use it is to collect and archive log data from both itself and the network machines it is monitoring. In addition to a machine which collects log data, all of the “source” machines being monitored will have to periodically send pertinent logs that they create to the “collector” machine. Moreover, the transmission of logs should be encrypted as well as follow an assortment of authentication policies to “Harden” the collection of event logs against malicious activity (NSA/CSS, 2013). Windows OS already has built-in features that allow for the logging of events and for their transmission to a collector device; and by isolating important logs on an otherwise unused collector machine, the risks of those logs being erased to hide nefarious activity is reduced and the benefits of logging as a way to detect vulnerabilities can be achieved (NSA/CSS, 2013).

References

Arpaci-Dusseau, R. & Arpaci-Dusseau, A. (2012). *Operating Systems: Three Easy Pieces.* Madison, WI: University of Wisconsin-Madison. Retrieved from <http://pages.cs.wisc.edu/~remzi/OSTEP//>

NSA/CSS (2013). Spotting the Adversary with Windows Event Log Monitoring, Revision 2. *United States of America National Security Agency.* Retrieved from <https://my.uopeople.edu/pluginfile.php/322781/mod_forum/attachment/3094792/U8%20Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf>