Project 3: Lock Down

Cyber Operations and Risk Management

Team 2 – Australia

CYB 670 Capstone in Cybersecurity

University of Maryland University College

Cyber Operations and Risk Management

The level of advanced technology that is essentially demanded by today’s society for ease of access to everyday actions has become a double-edged sword. Yes, being technically advanced is great, but comes with a serious liability, which is a nefarious actor whose technical abilities tend to be beyond advanced. With this risk brings a new set of challenges of being able to create cybersecurity policies that can mitigate or defeat this level of threat. A major challenge for any organization will be ensuring quality software assurance.

 Software assurance is a means of instilling confidence that software and services are free from intentional and unintentional vulnerabilities and that the software must also perform as intended. Expectations for the Australian Government governments computer network within the FVEY economic summit can essentially be broken down into 4 rules. Avoid installing any software which has malware pre-installed. Make sure that no vulnerabilities or exploitable parts of the source code are in the code prior to having the software accepted for operations. Make sure that future discoveries of any common vulnerabilities and exposures can be readily patched. Finally, ensure that the exploitable software that puts the stakeholder most at risk is mitigated before it is accepted for operations

Software assurance is proactive and plays an important role in every step of the Software Development Life Cycle. The Software Development Life Cycle is a systematic process utilized by the software industry to design, develop and test quality software, and their aim is to produce high quality software that meets or exceeds customers’ expectations. The SDLC identifies the process involved from the initial survey to the final maintenance of the developed application or software. It comprises a thorough plan describing how to develop, maintain, replace, alter or enhance specific software. There are some key attributes of SDLC which ensures that the process works in an efficiently and smooth. Each phase performs a significant role towards the development of the overall system. The seven phases are as follows: Planning, System Analysis, System Design, Development, Testing, Deployment/Implementation, and maintenance. The effort used to establish an information system is usually surpassed by the efforts required for the maintenance of the system, which can cost a lot of money and time. 50 to 60 percent of a major organizations is going to be tied up with maintenance on the systems.

The Software supply chain has the potential to be considered a major security risk. Each piece of the equipment may have multiple components sourced from various countries around the world. Some companies in foreign nations, such as China, are known for producing electronic components. This could pose a potential risk due to their ability to insert physical or software vulnerabilities into their components. Additionally, there is always the potential for tampering in transit, many devices are shipped via cargo vessel which spend weeks to months out at sea. There is plenty of time from the end of the manufacturing line to the receiving destination when an individual may attempt to tamper with a device. With no mitigation, this risk is inherited from every level in the supply chain as well as the final service or product increasing its likelihood for a security compromise.

Being able to understand the vulnerabilities and the inherent risks of a system is critical to the confidentiality of the data and stability of the overall system. All networks are essentially at risk from malicious nation-state actors, who tend to have a wide variety of motives and what seems to be unlimited techniques. A network such as the Australian Government, which is known to contain sensitive information is at a greater risk to face off with highly motivated and determined adversary. Vulnerabilities are the absence or weakness in safeguards within a network that can be exploited. It was discovered that the United States network during the FVEY’s Summit had vulnerabilities which ultimately left it exposed to the possibility of it being hit by the following types of attacks. Distributed Denial of Service (DDoS), Man-in-the-Middle attacks, Malware gaining access to the network, and finally phishing emails or links, that work off of the probability of human error.

Defining the software options that are going to meet or exceed our organizations requirements can become a daunting task. Especially when dealing with a technically advanced adversary, whose cyber-attack abilities tend to advance faster than our own defensive mechanisms. Which is a key factor as to why it is critical to ensure that our security software remains the most relevant and up to date as possible. Therefore, it is recommended that we start utilizing Endpoint security software. This security software is a much broader concept including not just antivirus software, but numerous security tools imbedded within, including, Firewalls, HIPS system, White Listing tools, as well as Patching and Logging tools. All of these tools work within one program in order to safeguard the various endpoints of an organization (as well as the organization itself against these endpoints) and from numerous other forms of security threats.

Before any of the previously mentioned recommendations can be implemented, there needs to be a general understanding that there is a cost associated to these improvements. There are times within any organization when it is appropriate to go with the lowest priced product that can meet your minimal viable product, security software is not that time. You get what you pay for. Now that does not mean go out and purchase the most expensive software there is and think that your system is 100% secure. A logical approach needs to happen. It is also important to note there will be licensing fees associated to the software, and those fees are based off the total number of devices required to have the software installed.