OLD DOMINION UNIVERSITY
CYSE 494

Proposal

Madelene McFarlane

10/9/2023

#01096496

In the modern-day technology is no longer considered just a tool in everyday life but a crucial factor in the overall operations on how we all function. Bank accounts, shopping, communication, and even education rely on technology and the networks that keep us all connected. While technology has allowed businesses and the ease of life to grow it has also grown the number security risks that one can face. Identity theft, scams, hacks, data leaks, and much more are now higher then ever in terms of threats and cybercrimes that the everyday person can experience. These risks being invited in by what is known as vulnerabilities be it through a network, software, or the user themselves. While human error is a critical vulnerability most vulnerabilities are more technical in nature and therefore hidden from less tech-savvy people or people that know how to use technology at a base level and can not keep track of all the details. To help ease this problem we are proposing the innovation of a new software technology that will offer services to help keep those safe and secure from vulnerabilities that could then leave them at risk of a cyberattack.

The problem at hand is more than just 'stopping an attack' or 'eliminating a cybercrime' it is the discussion of hidden vulnerabilities within a network that could potentially be exploited by someone wanting to do harm to an individual or a company. This is a problem that can be compared to that of a house. When a house has its front door unlocked that is not necessarily saying that the house will be broken into, but the risk of such a thing is increased due to that factor. An unlocked door being a vulnerability and the house being the network or system that one relies on. While an unlocked front door is a common understood risk, just like password health, a 3-pin keycode lock on a front door that has not been changed in ten years is a vulnerability that people often overlook or do not even see. What our innovation plans to accomplish is an easy, quick, and little technical knowledge required solution to the discovery of the vulnerabilities that a system holds.

The software in development would be similar in comparison to a malware scan. Though instead of scanning for malicious code it would be targeting vulnerabilities on a system. Therefore, factors such as updates waiting for installation, weak passwords, bugged code, UPAP enabled features, and more. Providing the user with a report to review of the vulnerabilities the system had and recommended actions. Along with the ability to auto start features as soon as the vulnerability is detected along with the implementation of auto scans so that way the user does not even have to think about manually starting a vulnerability scan. The auto start feature accompanying this by allowing the user to chose which fixes they would like to have automatically applied once detected. For example, if someone is using their computer and the auto scan goes through its normal cycle and discovers that there is a pending Windows update the user could enable auto start. This feature then kicking into effect as soon as the vulnerability is discovered and installing the Windows update.

Additional benefits to the program would include ability to further train staff members on computer and network safety as a result of their scans. Such as if a user's report comes back that

they have not updated their network password in a year. This information can then be built on top on as a learning opportunity on why it is important to regularly update important passwords due to factors like data leaks and blunt force attacks. This software would provide help to the proactive side of cybersecurity instead of the more come software of this nature that deal with the reactive side of cyberattacks and malware intrusions.

Though the software is built from the ground up to be of a helpful factor to people there are foreseeable barriers that this software might face. The software might be a learning curve to some users and therefore very through and simple worded explanations will be provided in regard to the services and recommendations the software provides. Along with suggestions of contacting partnered tech companies to help walk the user through the program in case a professional is needed to ensure proper implementation of the program. Additional barriers that are to be expected are licensing and legal issues since this code will require administrative privileges to function. Therefore, leaving the software liable to accusations of breaching sensitive information due to needing administrative privileges even though the software will never send or use the data maliciously against the user.

With the continued rise of technology in everyday life as well as businesses proceeding to grow with technology. The crime behind technology grows as well because of all the valuable information that is now being stored and transferred through our systems. While the growing education of reactive measures is well covered the proactive side is left with little padding. In order for a hack to successfully go through a system the malicious action first needs a vulnerability to exploit. The vulnerability is where our product would come in to play. Providing users with a scanned report of the vulnerabilities that are within their system along with the proper steps required in order to neutralize them. This in turn locking the front door of the house in order to prevent and lower the risk of intruders walking in the front door.

This software would be a success because of its ability to ease the manual requirements needed to keep all vulnerabilities checked and up to date. The software being used in a variety of different ways. The first way being that of a proactive protection software for businesses and for personal computer systems. The second way is that the generated report can serve as a training tool for the administration and user as to why and how this vulnerability can be fixed and the importance of keeping this vulnerability patched. Lastly, this software can provide as a tool to tech companies that offer outsourcing of their own technicians. Our product being an excellent addition to their toolbelt and therefore their overall service to their client. The ability to scan through a system and being fed a report of all the holes that increase the risk of a breach making for a more efficient workflow for both tech companies, businesses, and those looking out for their own cyber protection. With a wide range of benefits and uses apart of the growing influx of technology this software would be successful to more people then every before.