Tyler Kim
Intro to Cybersecurity
Word Count: 372

Policy Homework

It is said, “security isn’t something you buy, it’s something you do”. As the quote correctly states, the user determines how secure a system is through good habits and their security awareness behavior. Therefore, I propose that government and essential business computer systems stay current and updated. I assume that government officials undergo some sort of security awareness training and that computer systems have basic security protocols such as password complexity, password duration, a firewall, and many others. In addition, I can assume that government and essential business technology tend to be a few years behind. There are multiple reasons why my proposal would be effective.

My proposal essentially requires that government and essential business IT teams update their systems to the latest update to protect individuals’ private information. Oftentimes, government and essential businesses’ computer systems tend to be a few years behind making their systems vulnerable. Especially hospital systems are prime targets for personal data and are susceptible to exploits. For example, the WannaCry ransomware targeted around 300,000 machines in 150 countries, in fact, outdated hospital systems contributed to the spread of the ransomware. Such attacks prevent doctors and nurses from accessing medical data for patients putting them at risk. If hospital computer systems or any essential businesses and government’s computer systems were updated, the impact of a ransomware such as WannaCry would be mitigated.

In addition, my proposal implies that government and essential businesses update their applications to reduce the chances and the impact of the exploit. Updating applications, especially ones that have access to sensitive data, patches loopholes and fixes possible vulnerabilities making computer systems more secure. Techniques such as cross site scripting, SQL injections, and many others become less effective since more loopholes are patched. Finally, keeping government and essential businesses’ computer systems updated allows greater compatibility with other software. New technologies are often built with newer tools and software which means that they tend to be incompatible with older applications because older applications may not have the required feature for a new technology to run properly. Similarly, it makes sense that the government and essential businesses keep their computer systems updated to take advantage of new technology and stay caught up with the rapid development of technology.

References

https://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html

https://www.veracode.com/security/application-security-vulnerability-code-flaws-insecure-code